KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
HENRY C. BUNSOW - #60707
MICHAEL H. PAGE - #154913
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

INTERTRUST TECHNOLOGIES CORPORATION
DOUGLAS K. DERWIN - #111407
MARK SCADINA - #173103
JEFF MCDOW - #184727
4800 Patrick Henry Drive
Santa Clara, CA 95054
Telephone: (408) 855-0100
Facsimile: (408) 855-0144

Attorneys for Plaintiff and Counter-Defendant
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant. AND COUNTER ACTION.	Case No. C 01-1640 SBA (MEJ) Consolidated with C 02-0647 SBA **FOURTH AMENDED COMPLAINT FOR INFRINGEMENT OF U.S. PATENT NOS. 6,185,683 B1; 6,253,193 B1; 5,920,861; 5,892,900; 5,982,891; 5,917,912; 6,157,721; 5,915,019; 5,949,876; 6,112,181; AND 6,389,402 B1.** **DEMAND FOR JURY TRIAL**

Plaintiff INTERTRUST TECHNOLOGIES CORPORATION (hereafter "InterTrust")

hereby complains of Defendant MICROSOFT CORPORATION (hereafter "Microsoft"), and

alleges as follows:

JURISDICTION AND VENUE

1.   This action for patent infringement arises under the patent laws of the United

States, Title 35, United States Code, more particularly 35 U.S.C. §§ 271 and 281.

2. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(c) and 1400(b).

THE PARTIES

4. Plaintiff InterTrust is a Delaware corporation with its principal place of business at 4750 Patrick Henry Drive, Santa Clara, California.

5. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft is a Washington Corporation with its principal place of business at One Microsoft Way, Redmond, Washington.

6. InterTrust is informed and believes, and on that basis alleges, that Defendant Microsoft does business in this judicial district and has committed and is continuing to commit acts of infringement in this judicial district.

7. InterTrust is the owner of United States Patent No. 6,185,683 B1, entitled "Trusted and secure techniques, systems and methods for item delivery and execution" ("the '683 patent"), duly and lawfully issued on February 6, 2001.

8. InterTrust is the owner of United States Patent No. 6,253,193 B1, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '193 patent"), duly and lawfully issued on June 26, 2001.

9. InterTrust is the owner of United States Patent No. 5,920,861, entitled "Techniques for defining, using and manipulating rights management data structures" ("the '861 patent"), duly and lawfully issued on July 6, 1999.

10. InterTrust is the owner of United States Patent No. 5,892,900, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '900 patent"), duly and lawfully issued on April 6, 1999.

11. InterTrust is the owner of United States Patent No. 5,982,891, entitled "Systems and methods for secure transaction management and electronic rights protection" ("the '891 patent"), duly and lawfully issued on November 9, 1999.

12. InterTrust is the owner of United States Patent No. 5,917,912 entitled "System

2

1   and methods for secure transaction management and electronic rights protection" ("the '912

2   patent"), duly and lawfully issued on June 29, 1999.

3   13.   InterTrust is the owner of United States Patent No. 6,157,721, entitled "Systems

4   and methods using cryptography to protect secure computing environments" ("the '721 patent"),

5   duly and lawfully issued on December 5, 2000.

6   14.   InterTrust is the owner of United States Patent No. 5,915,019, entitled "Systems

7   and methods for secure transaction management and electronic rights protection" (the '019

8   patent"), duly and lawfully issued on June 22, 1999.

9   15.   InterTrust is the owner of United States Patent No. 5,949,876, entitled "Systems

10 and methods for secure transaction management and electronic rights protection" ("the '876

11 patent"), duly and lawfully issued on September 7, 1999.

12   16.   InterTrust is the owner of United States Patent No. 6,112,181, entitled "Systems

13 and methods for matching, selecting, narrowcasting, and/or classifying based on rights

14 management and/or other information" ("the '181 patent"), duly and lawfully issued on August

15 29, 2000.

16   17.   InterTrust is the owner of United States Patent No. 6,389,402 B1, entitled

17 "Systems and methods for secure transaction management and electronic rights protection" ("the

18 '402 patent"), duly and lawfully issued on May 14, 2002.

19   **FIRST CLAIM FOR RELIEF**

20   18.   InterTrust hereby incorporates by reference paragraphs 1-7 as if restated herein.

21   19.   This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

22   20.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

23 been and is infringing the '683 patent under § 271(a), as identified in InterTrust's Patent Local

24 Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and

25 belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the

26 process of developing other systems, which infringe the '683 patent under § 271(a). InterTrust is

27 further informed and believes, and on that basis alleges, that Microsoft's infringement of the

28 '683 patent under § 271(a) will continue unless enjoined by this Court.

FOURTH AMENDED COMPLAINT FOR INFRINGEMENT OF U.S. PATENTS
CASE NO. C 01-1640 SBA (MED) CONSOLIDATED WITH C 02-0647 SBA

21. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '683 patent under § 271(a), thereby inducing infringement of the '683 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under § 271(b) will continue unless enjoined by this Court.

22. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '683 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '683 patent under § 271(c) will continue unless enjoined by this Court.

23. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '683 patent in the manner described above in paragraphs 20 through 22, and will continue to do so unless enjoined by this Court.

24. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

SECOND CLAIM FOR RELIEF

25. InterTrust hereby incorporates by reference paragraphs 1-6 and 8 as if restated herein.

26. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

4

300566.01

27. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '193 patent under § 271(a), as identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '193 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under § 271(a) will continue unless enjoined by this Court.

28. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '193 patent under § 271(a), thereby inducing infringement of the '193 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under § 271(b) will continue unless enjoined by this Court.

29. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '193 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '193 patent under § 271(c) will continue unless enjoined by this Court.

30. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '193 patent in the manner described above in paragraphs 27 through 29, and will continue to do so unless enjoined by this Court.

31. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of

300568.01

1   infringement gains, profits, and advantages, tangible and intangible, the extent of which are not

2   presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has

3   been, and will continue to be, irreparably harmed.

THIRD CLAIM FOR RELIEF

5   32.   InterTrust hereby incorporates by reference paragraphs 1-6 and 9 as if restated

6   herein.

7   33.   This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

8   34.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

9   been and is infringing the '861 patent under § 271(a), as identified in InterTrust's Patent Local

10   Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and

11   belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the

12   process of developing other systems, which infringe the '861 patent under § 271(a). InterTrust is

13   further informed and believes, and on that basis alleges, that Microsoft's infringement of the

14   '861 patent under § 271(a) will continue unless enjoined by this Court.

15   35.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

16   been and is knowingly and intentionally inducing others to infringe directly the '861 patent under

17   § 271(a), thereby inducing infringement of the '861 patent under § 271(b). InterTrust is further

18   informed and believes that Microsoft's inducement has at least included the manner in which

19   Microsoft has promoted and marketed use of its software and services identified in InterTrust's

20   Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further

21   informed and believes, and on that basis alleges, that Microsoft's infringement of the '861 patent

22   under § 271(b) will continue unless enjoined by this Court.

23   36.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

24   been and is contributorily infringing the '861 patent under § 271(c) by providing software and

25   services especially made or especially adapted for infringing use and not staple articles or

26   commodities of commerce suitable for substantial noninfringing use, including at least the

27   software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on

28   Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis

6

FOURTH AMENDED COMPLAINT FOR INFRINGEMENT OF U.S. PATENTS
CASE NO. C 01-1640 SBA (AMEND. CONSOLIDATED WITH C 02-0647 SBA

1   alleges, that Microsoft's infringement of the '861 patent under § 271(c) will continue unless

2   enjoined by this Court.

3   37.   InterTrust is informed and believes, and on that basis alleges, that Microsoft is

4   willfully infringing the '861 patent in the manner described above in paragraphs 34 through 36,

5   and will continue to do so unless enjoined by this Court.

6   38.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

7   derived and received, and will continue to derive and receive from the aforesaid acts of

8   infringement gains, profits, and advantages, tangible and intangible, the extent of which are not

9   presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has

10   been, and will continue to be, irreparably harmed.

11   **FOURTH CLAIM FOR RELIEF**

12   39.   InterTrust hereby incorporates by reference paragraphs 1-6 and 10 as if restated

13   herein.

14   40.   This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

15   41.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

16   been and is infringing the '900 patent under § 271(a), as identified in InterTrust's Patent Local

17   Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and

18   belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the

19   process of developing other systems, which infringe the '900 patent under § 271(a). InterTrust is

20   further informed and believes, and on that basis alleges, that Microsoft's infringement of the

21   '900 patent under § 271(a) will continue unless enjoined by this Court.

22   42.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

23   been and is knowingly and intentionally inducing others to infringe directly the '900 patent under

24   § 271(a), thereby inducing infringement of the '900 patent under § 271(b). InterTrust is further

25   informed and believes that Microsoft's inducement has at least included the manner in which

26   Microsoft has promoted and marketed use of its software and services identified in InterTrust's

27   Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further

28   informed and believes, and on that basis alleges, that Microsoft's infringement of the '900 patent

300566.01

1   under § 271(b) will continue unless enjoined by this Court.

2   43.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

3   been and is contributorily infringing the '900 patent under § 271(c) by providing software and

4   services especially made or especially adapted for infringing use and not staple articles or

5   commodities of commerce suitable for substantial noninfringing use, including at least the

6   software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on

7   Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis

8   alleges, that Microsoft's infringement of the '900 patent under § 271(c) will continue unless

9   enjoined by this Court.

10   44.   InterTrust is informed and believes, and on that basis alleges, that Microsoft is

11 willfully infringing the '900 patent in the manner described above in paragraphs 41 through 43,

12 and will continue to do so unless enjoined by this Court.

13   45.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

14 derived and received, and will continue to derive and receive from the aforesaid acts of

15 infringement gains, profits, and advantages, tangible and intangible, the extent of which are not

16 presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has

17 been, and will continue to be, irreparably harmed.

18   **FIFTH CLAIM FOR RELIEF**

19   46.   InterTrust hereby incorporates by reference paragraphs 1-6 and 11 as if restated

20 herein.

21   47.   This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

22   48.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

23 been and is infringing the '891 patent under § 271(a), as identified in InterTrust's Patent Local

24 Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and

25 belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the

26 process of developing other systems, which infringe the '891 patent under § 271(a). InterTrust is

27 further informed and believes, and on that basis alleges, that Microsoft's infringement of the

28 '891 patent under § 271(a) will continue unless enjoined by this Court.

8

49.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '891 patent under § 271(a). thereby inducing infringement of the '891 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '891 patent under § 271(b) will continue unless enjoined by this Court.

50.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '891 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '891 patent under § 271(c) will continue unless enjoined by this Court.

51.   InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '891 patent in the manner described above in paragraphs 48 through 50, and will continue to do so unless enjoined by this Court.

52.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

SIXTH CLAIM FOR RELIEF

53.   InterTrust hereby incorporates by reference paragraphs 1-6 and 12 as if restated herein.

54.   This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

9

300566.01

1   55.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

2 been and is infringing the '912 patent under § 271(a), as identified in InterTrust's Patent Local

3 Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and

4 belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the

5 process of developing other systems, which infringe the '912 patent under § 271(a). InterTrust is

6 further informed and believes, and on that basis alleges, that Microsoft's infringement of the

7 '912 patent under § 271(a) will continue unless enjoined by this Court.

8   56.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

9 been and is knowingly and intentionally inducing others to infringe directly the '912 patent under

10 § 271(a), thereby inducing infringement of the '912 patent under § 271(b). InterTrust is further

11 informed and believes that Microsoft's inducement has at least included the manner in which

12 Microsoft has promoted and marketed use of its software and services identified in InterTrust's

13 Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further

14 informed and believes, and on that basis alleges, that Microsoft's infringement of the '912 patent

15 under § 271(b) will continue unless enjoined by this Court.

16   57.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

17 been and is contributorily infringing the '912 patent under § 271(c) by providing software and

18 services especially made or especially adapted for infringing use and not staple articles or

19 commodities of commerce suitable for substantial noninfringing use, including at least the

20 software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on

21 Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis

22 alleges, that Microsoft's infringement of the '912 patent under § 271(c) will continue unless

23 enjoined by this Court.

24   58.   InterTrust is informed and believes, and on that basis alleges, that Microsoft is

25 willfully infringing the '912 patent in the manner described above in paragraphs 55 through 57,

26 and will continue to do so unless enjoined by this Court.

27   59.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

28 derived and received, and will continue to derive and receive from the aforesaid acts of

10

300566.01

1 infringement gains, profits, and advantages, tangible and intangible, the extent of which are not

2 presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has

3 been, and will continue to be, irreparably harmed.

4 ## SEVENTH CLAIM FOR RELIEF

5   60.   InterTrust hereby incorporates by reference paragraphs 1-6 and 13 as if restated

6 herein.

7   61..   This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

8   62.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

9 been and is infringing the '721 patent under § 271(a), as identified in InterTrust's Patent Local

10 Rule 3-1 disclosures served on Microsoft on June 21, 2002. In addition, on information and

11 belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the

12 process of developing other systems, which infringe the '721 patent under § 271(a). InterTrust is

13 further informed and believes, and on that basis alleges, that Microsoft's infringement of the

14 '721 patent under § 271(a) will continue unless enjoined by this Court.

15   63.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

16 been and is knowingly and intentionally inducing others to infringe directly the '721 patent under

17 § 271(a), thereby inducing infringement of the '721 patent under § 271(b). InterTrust is further

18 informed and believes that Microsoft's inducement has at least included the manner in which

19 Microsoft has promoted and marketed use of its software and services identified in InterTrust's

20 Patent Local Rule 3-1 disclosures served on Microsoft on June 21, 2002. InterTrust is further

21 informed and believes, and on that basis alleges, that Microsoft's infringement of the '721 patent

22 under § 271(b) will continue unless enjoined by this Court.

23   64.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

24 been and is contributorily infringing the '721 patent under § 271(c) by providing software and

25 services especially made or especially adapted for infringing use and not staple articles or

26 commodities of commerce suitable for substantial noninfringing use, including at least the

27 software and services identified in InterTrust's Patent Local Rule 3-1 disclosures served on

28 Microsoft on June 21, 2002.. InterTrust is further informed and believes, and on that basis

1   alleges, that Microsoft's infringement of the '721 patent under § 271(c) will continue unless

2   enjoined by this Court.

3   65.   InterTrust is informed and believes, and on that basis alleges, that Microsoft is

4   willfully infringing the '721 patent in the manner described above in paragraphs 62 through 64,

5   and will continue to do so unless enjoined by this Court.

6   66.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

7   derived and received, and will continue to derive and receive from the aforesaid acts of

8   infringement gains, profits, and advantages, tangible and intangible, the extent of which are not

9   presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has

10 been, and will continue to be, irreparably harmed.

EIGHTH CLAIM FOR RELIEF

12   67.   InterTrust hereby incorporates by reference paragraphs 1-6 and 14 as if restated

13 herein.

14   68.   This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

15   69.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

16 been and is infringing the '019 patent under § 271(a), as identified in InterTrust's Draft Claim

17 Charts presented to Microsoft on June 21, 2002. In addition, on information and belief,

18 InterTrust alleges that Microsoft is making and using other systems and/or is in the process of

19 developing other systems, which infringe the '019 patent under § 271(a). InterTrust is further

20 informed and believes, and on that basis alleges, that Microsoft's infringement of the '019 patent

21 under § 271(a) will continue unless enjoined by this Court.

22   70.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

23 been and is knowingly and intentionally inducing others to infringe directly the '019 patent under

24 § 271(a), thereby inducing infringement of the '019 patent under § 271(b). InterTrust is further

25 informed and believes that Microsoft's inducement has at least included the manner in which

26 Microsoft has promoted and marketed use of its software and services identified in InterTrust's

27 Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and

28 believes, and on that basis alleges, that Microsoft's infringement of the '019 patent under §

1 271(b) will continue unless enjoined by this Court.

2   71.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

3 been and is contributorily infringing the '019 patent under § 271(c) by providing software and

4 services especially made or especially adapted for infringing use and not staple articles or

5 commodities of commerce suitable for substantial noninfringing use, including at least the

6 software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on

7 June 21. 2002.. InterTrust is further informed and believes, and on that basis alleges, that

8 Microsoft's infringement of the '019 patent under § 271(c) will continue unless enjoined by this

9 Court.

10   72.   InterTrust is informed and believes, and on that basis alleges, that Microsoft is

11 willfully infringing the '019 patent in the manner described above in paragraphs 69 through 71,

12 and will continue to do so unless enjoined by this Court.

13   73.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

14 derived and received, and will continue to derive and receive from the aforesaid acts of

15 infringement gains, profits, and advantages, tangible and intangible, the extent of which are not

16 presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has

17 been, and will continue to be, irreparably harmed.

18   **NINTH CLAIM FOR RELIEF**

19   74.   InterTrust hereby incorporates by reference paragraphs 1-6 and 15 as if restated

20 herein.

21   75.   This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

22   76.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

23 been and is infringing the '876 patent under § 271(a), as identified in InterTrust's Draft Claim

24 Charts presented to Microsoft on June 21, 2002. In addition, on information and belief,

25 InterTrust alleges that Microsoft is making and using other systems and/or is in the process of

26 developing other systems, which infringe the '876 patent under § 271(a). InterTrust is further

27 informed and believes, and on that basis alleges, that Microsoft's infringement of the '876 patent

28 under § 271(a) will continue unless enjoined by this Court.

13

77. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '876 patent under § 271(a), thereby inducing infringement of the '876 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '876 patent under § 271(b) will continue unless enjoined by this Court.

78. InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '876 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '876 patent under § 271(c) will continue unless enjoined by this Court.

79. InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '876 patent in the manner described above in paragraphs 76 through 78, and will continue to do so unless enjoined by this Court.

80. InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of infringement gains, profits, and advantages, tangible and intangible, the extent of which are not presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has been, and will continue to be, irreparably harmed.

TENTH CLAIM FOR RELIEF

81. InterTrust hereby incorporates by reference paragraphs 1-6 and 16 as if restated herein.

82. This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

14

83.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is infringing the '181 patent under § 271(a), as identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. In addition, on information and belief, InterTrust alleges that Microsoft is making and using other systems and/or is in the process of developing other systems, which infringe the '181 patent under § 271(a). InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '181 patent under § 271(a) will continue unless enjoined by this Court.

84.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is knowingly and intentionally inducing others to infringe directly the '181 patent under § 271(a), thereby inducing infringement of the '181 patent under § 271(b). InterTrust is further informed and believes that Microsoft's inducement has at least included the manner in which Microsoft has promoted and marketed use of its software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '181 patent under § 271(b) will continue unless enjoined by this Court.

85.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has been and is contributorily infringing the '181 patent under § 271(c) by providing software and services especially made or especially adapted for infringing use and not staple articles or commodities of commerce suitable for substantial noninfringing use, including at least the software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that Microsoft's infringement of the '181 patent under § 271(c) will continue unless enjoined by this Court.

86.   InterTrust is informed and believes, and on that basis alleges, that Microsoft is willfully infringing the '181 patent in the manner described above in paragraphs 83 through 85, and will continue to do so unless enjoined by this Court.

87.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has derived and received, and will continue to derive and receive from the aforesaid acts of

15

300588.01

1   infringement gains, profits, and advantages, tangible and intangible, the extent of which are not

2   presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has

3   been, and will continue to be, irreparably harmed.

ELEVENTH CLAIM FOR RELIEF

5   88.   InterTrust hereby incorporates by reference paragraphs 1-6 and 17 as if restated

6   herein.

7   89.   This is a claim for patent infringement under 35 U.S.C. §§ 271 and 281.

8   90.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

9   been and is infringing the '402 patent under § 271(a), as identified in InterTrust's Draft Claim

10 Charts presented to Microsoft on June 21, 2002. In addition, on information and belief,

11 InterTrust alleges that Microsoft is making and using other systems and/or is in the process of

12 developing other systems, which infringe the '402 patent under § 271(a). InterTrust is further

13 informed and believes, and on that basis alleges, that Microsoft's infringement of the '402 patent

14 under § 271(a) will continue unless enjoined by this Court.

15 91.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

16 been and is knowingly and intentionally inducing others to infringe directly the '402 patent under

17 § 271(a), thereby inducing infringement of the '402 patent under § 271(b). InterTrust is further

18 informed and believes that Microsoft's inducement has at least included the manner in which

19 Microsoft has promoted and marketed use of its software and services identified in InterTrust's

20 Draft Claim Charts presented to Microsoft on June 21, 2002. InterTrust is further informed and

21 believes, and on that basis alleges, that Microsoft's infringement of the '402 patent under §

22 271(b) will continue unless enjoined by this Court.

23 92.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

24 been and is contributorily infringing the '402 patent under § 271(c) by providing software and

25 services especially made or especially adapted for infringing use and not staple articles or

26 commodities of commerce suitable for substantial noninfringing use, including at least the

27 software and services identified in InterTrust's Draft Claim Charts presented to Microsoft on

28 June 21, 2002. InterTrust is further informed and believes, and on that basis alleges, that

16

300566.01

1 Microsoft's infringement of the '402 patent under § 271(c) will continue unless enjoined by this

2 Court.

3   93.   InterTrust is informed and believes, and on that basis alleges, that Microsoft is

4 willfully infringing the '402 patent in the manner described above in paragraphs 90 through 92,

5 and will continue to do so unless enjoined by this Court.

6   94.   InterTrust is informed and believes, and on that basis alleges, that Microsoft has

7 derived and received, and will continue to derive and receive from the aforesaid acts of

8 infringement gains, profits, and advantages, tangible and intangible, the extent of which are not

9 presently known to InterTrust. By reason of the aforesaid acts of infringement, InterTrust has

10 been, and will continue to be, irreparably harmed.

11 <div align="center">PRAYER FOR RELIEF</div>

12   WHEREFORE, InterTrust prays for relief as follows:

13   A.   That Microsoft be adjudged to have infringed the '683 patent under 35 U.S.C. §

14 271(a);

15   B.   That Microsoft be adjudged to have infringed the '683 patent under 35 U.S.C. §

16 271(b) by inducing others to infringe directly the '683 patent under 35 U.S.C. § 271(a);

17   C.   That Microsoft be adjudged to have contributorily infringed the '683 patent under

18 35 U.S.C. § 271(c);

19   D.   That Microsoft be adjudged to have willfully infringed the '683 patent under 35

20 U.S.C. §§ 271(a), (b), and (c);

21   E.   That Microsoft, its officers, agents, servants, employees and attorneys, and those

22 persons in active concert or participation with them be preliminarily and permanently restrained

23 and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '683 patent;

24   F.   That Microsoft be adjudged to have infringed the '193 patent under 35 U.S.C. §

25 271(a);

26   G.   That Microsoft be adjudged to have infringed the '193 patent under 35 U.S.C. §

27 271(b) by inducing others to infringe directly the '193 patent under 35 U.S.C. § 271(a);

28 ///

<div align="center">17</div>

1   H.   That Microsoft be adjudged to have contributorily infringed the '193 patent under

2 35 U.S.C. § 271(c);

3   I.   That Microsoft be adjudged to have willfully infringed the '193 patent under 35

4 U.S.C. §§ 271(a), (b), and (c);

5   J.   That Microsoft, its officers, agents, servants, employees and attorneys, and those

6 persons in active concert or participation with them be preliminarily and permanently restrained

7 and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '193 patent;

8   K.   That Microsoft be adjudged to have infringed the '861 patent under 35 U.S.C. §

9 271(a);

10   L.   That Microsoft be adjudged to have infringed the '861 patent under 35 U.S.C. §

11 271(b) by inducing others to infringe directly the '861 patent under 35 U.S.C. § 271(a);

12   M.   That Microsoft be adjudged to have contributorily infringed the '861 patent under

13 35 U.S.C. § 271(c);

14   N.   That Microsoft be adjudged to have willfully infringed the '861 patent under 35

15 U.S.C. §§ 271(a), (b), and (c);

16   O.   That Microsoft, its officers, agents, servants, employees and attorneys, and those

17 persons in active concert or participation with them be preliminarily and permanently restrained

18 and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '861 patent;

19   P.   That Microsoft be adjudged to have infringed the '900 patent under 35 U.S.C. §

20 271(a);

21   Q.   That Microsoft be adjudged to have infringed the '900 patent under 35 U.S.C. §

22 271(b) by inducing others to infringe directly the '900 patent under 35 U.S.C. § 271(a);

23   R.   That Microsoft be adjudged to have contributorily infringed the '900 patent under

24 35 U.S.C. § 271(c);

25   S.   That Microsoft be adjudged to have willfully infringed the '900 patent under 35

26 U.S.C. §§ 271(a), (b), and (c);

27   T.   That Microsoft, its officers, agents, servants, employees and attorneys, and those

28 persons in active concert or participation with them be preliminarily and permanently restrained

1 and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '900 patent;

2 U.   That Microsoft be adjudged to have infringed the '891 patent under 35 U.S.C. §

3 271(a);

4 V.   That Microsoft be adjudged to have infringed the '891 patent under 35 U.S.C. §

5 271(b) by inducing others to infringe directly the '891 patent under 35 U.S.C. § 271(a);

6 W.   That Microsoft be adjudged to have contributorily infringed the '891 patent under

7 35 U.S.C. § 271(c);

8 X.   That Microsoft be adjudged to have willfully infringed the '891 patent under 35

9 U.S.C. §§ 271(a), (b), and (c);

10 Y.   That Microsoft, its officers, agents, servants, employees and attorneys, and those

11 persons in active concert or participation with them be preliminarily and permanently restrained

12 and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '891 patent;

13 Z.   That Microsoft be adjudged to have infringed the '912 patent under 35 U.S.C. §

14 271(a);

15 AA.   That Microsoft be adjudged to have infringed the '912 patent under 35 U.S.C. §

16 271(b) by inducing others to infringe directly the '912 patent under 35 U.S.C. § 271(a);

17 BB.   That Microsoft be adjudged to have contributorily infringed the '912 patent under

18 35 U.S.C. § 271(c);

19 CC.   That Microsoft be adjudged to have willfully infringed the '912 patent under 35

20 U.S.C. §§ 271(a), (b), and (c);

21 DD.   That Microsoft, its officers, agents, servants, employees and attorneys, and those

22 persons in active concert or participation with them be preliminarily and permanently restrained

23 and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '912 patent;

24 EE.   That Microsoft be adjudged to have infringed the '721 patent under 35 U.S.C. §

25 271(a);

26 FF.   That Microsoft be adjudged to have infringed the '721 patent under 35 U.S.C. §

27 271(b) by inducing others to infringe directly the '721 patent under 35 U.S.C. § 271(a);

28 ///

19

1   GG.   That Microsoft be adjudged to have contributorily infringed the '721 patent under

2   35 U.S.C. § 271(c);

3   HH.   That Microsoft be adjudged to have willfully infringed the '721 patent under 35

4   U.S.C. §§ 271(a), (b), and (c);

5   II.   That Microsoft, its officers, agents, servants, employees and attorneys, and those

6   persons in active concert or participation with them be preliminarily and permanently restrained

7   and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '721 patent;

8   JJ.   That Microsoft be adjudged to have infringed the '019 patent under 35 U.S.C. §

9   271(a);

10   KK.   That Microsoft be adjudged to have infringed the '019 patent under 35 U.S.C. §

11   271(b) by inducing others to infringe directly the '019 patent under 35 U.S.C. § 271(a);

12   LL.   That Microsoft be adjudged to have contributorily infringed the '019 patent under

13   35 U.S.C. § 271(c);

14   MM.   That Microsoft be adjudged to have willfully infringed the '019 patent under 35

15   U.S.C. §§ 271(a), (b), and (c);

16   NN.   That Microsoft, its officers, agents, servants, employees and attorneys, and those

17   persons in active concert or participation with them be preliminarily and permanently restrained

18   and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '019 patent;

19   OO.   That Microsoft be adjudged to have infringed the '876 patent under 35 U.S.C. §

20   271(a);

21   PP.   That Microsoft be adjudged to have infringed the '876 patent under 35 U.S.C. §

22   271(b) by inducing others to infringe directly the '876 patent under 35 U.S.C. § 271(a);

23   QQ.   That Microsoft be adjudged to have contributorily infringed the '876 patent under

24   35 U.S.C. § 271(c);

25   RR.   That Microsoft be adjudged to have willfully infringed the '876 patent under 35

26   U.S.C. §§ 271(a), (b), and (c);

27   ///

28   ///

20

1   SS.   That Microsoft, its officers, agents, servants, employees and attorneys, and those

2   persons in active concert or participation with them be preliminarily and permanently restrained

3   and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '876 patent;

4   TT.   That Microsoft be adjudged to have infringed the '181 patent under 35 U.S.C. §

5   271(a);

6   UU.   That Microsoft be adjudged to have infringed the '181 patent under 35 U.S.C. §

7   271(b) by inducing others to infringe directly the '181 patent under 35 U.S.C. § 271(a);

8   VV.   That Microsoft be adjudged to have contributorily infringed the '181 patent under

9   35 U.S.C. § 271(c);

10   WW.   That Microsoft be adjudged to have willfully infringed the '181 patent under 35

11   U.S.C. §§ 271(a), (b), and (c);

12   XX.   That Microsoft, its officers, agents, servants, employees and attorneys, and those

13   persons in active concert or participation with them be preliminarily and permanently restrained

14   and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '181 patent;

15   YY.   That Microsoft be adjudged to have infringed the '402 patent under 35 U.S.C. §

16   271(a);

17   ZZ.   That Microsoft be adjudged to have infringed the '402 patent under 35 U.S.C. §

18   271(b) by inducing others to infringe directly the '402 patent under 35 U.S.C. § 271(a);

19   AAA.   That Microsoft be adjudged to have contributorily infringed the '402 patent under

20   35 U.S.C. § 271(c);

21   BBB.   That Microsoft be adjudged to have willfully infringed the '402 patent under 35

22   U.S.C. §§ 271(a), (b), and (c);

23   CCC.   That Microsoft, its officers, agents, servants, employees and attorneys, and those

24   persons in active concert or participation with them be preliminarily and permanently restrained

25   and enjoined under 35 U.S.C. § 283 from directly or indirectly infringing the '402 patent;

26   DDD.   That this Court award damages to compensate InterTrust for Microsoft's

27   infringement, as well as enhanced damages, pursuant to 35 U.S.C. § 284;

28   ///

300566.01

1   EEE.   That this Court adjudge this case to be exceptional and award reasonable

2 attorney's fees to InterTrust pursuant to 35 U.S.C. § 285;

3   FFF.   That this Court assess pre-judgment and post-judgment interest and costs against

4 Microsoft, and award such interest and costs to InterTrust, pursuant to 35 U.S.C. § 284; and

5   GGG.   That InterTrust have such other and further relief as the Court may deem proper.

6
   Dated: October 24, 2002   KEKER & VAN NEST, LLP
7
8   By:_____
                                         MICHAEL H. PAGE
9   Attorneys for Plaintiff and Counter
                                         Defendant
10   INTERTRUST TECHNOLOGIES
                                         CORPORATION
11

12

13   DEMAND FOR JURY TRIAL

14   Plaintiff InterTrust herby demands a trial by jury as to all issues triable by jury,

15 specifically including, but not limited to, the issue of infringement of United States Patent Nos.

16 6,185,683 B1; 6,253,193 B1; 5,920,861; 5,892,900; 5,982,891; 5,917,912; 6,157,721;

17 5,915,019; 5,949,876; 6,112,181; and 6,389,402 B1.

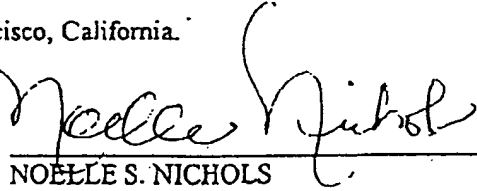18 Dated: October 24, 2002   KEKER & VAN NEST, LLP

19

20

21   By:_____
                                         MICHAEL H. PAGE
22   Attorneys for Plaintiff and Counter
                                         Defendant
23   INTERTRUST TECHNOLOGIES
                                         CORPORATION

24

25

26

27

28

                                    22

PROOF OF SERVICE

2 I am employed in the City and County of San Francisco, State of California in the office of a
member of the bar of this court at whose direction the following service was made. I am over the
3 age of eighteen years and not a party to the within action. My business address is Keker & Van
Nest, LLP, 710 Sansome Street, San Francisco, California 94111.

5 On October 24, 2002, I served the following document(s):

6 **FOURTH AMENDED COMPLAINT FOR INFRINGEMENT OF U.S. PATENT NOS.
6,185,683 B1; 6,253,193 B1; 5,920,861; 5,892,900; 5,982,891; 5,917,912; 6,157,721;
7 5,915,019; 5,949,876; 6,112,181; AND 6,389,402 B1**

8 **DEMAND FOR JURY TRIAL**

10 ☑   by FACSIMILE TRANSMISSION (IKON) AND UNITED STATES MAIL, by placing a true and
correct copy with IKON Office Solutions, the firm's in-house facsimile transmission center provider, for
transmission on this date. The transmission was reported as complete and without error. A true and correct
11 copy of same was placed in a sealed envelope addressed as shown below. I am readily familiar with the
practice of Keker & Van Nest, LLP for collection and processing of correspondence for mailing.
12 According to that practice, items are deposited with the United States Postal Service at San Francisco,
California on that same day with postage thereon fully prepaid. I am aware that, on motion of the party
13 served, service is presumed invalid if the postal cancellation date or the postage meter date is more than one
day after the date of deposit for mailing stated in this affidavit.

14
Eric L Wesenberg, Esq.   John D. Vandenberg, Esq.
15 Mark R. Weinstein, Esq.   James E. Geringer, Esq.
Orrick Herrington & Sutcliffe   Kristin L. Cleveland, Esq.
16 1000 Marsh Road   Klarquist Sparkman Campbell, et al.
Menlo Park, CA 94025   One World Trade Center, Suite 1600
17 Telephone: 650/614-7400   121 S.W. Salmon Street
Facsimile: 650/614-7401   Portland OR 97204
18   Telephone: 503/226-7391
Facsimile: 503/228-9446
19

20 I declare under penalty of perjury under the laws of the State of California that the above is true
21 and correct.

22 Executed on October 24, 2002, at San Francisco, California.

23
24   _____
NOELLE S. NICHOLS
25

26

27

28

1

300566.01

ERIC L. WESENBERG (State Bar No. 139696)
SAM O'ROURKE (State Bar No. 205233)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

Attorneys for Defendant and Counterclaimant
MICROSOFT CORPORATION

RECEIVED

OCT 2 8 2002

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant. AND RELATED CROSS-ACTION.	Case No. C 01-1640 SBA (MEJ) [PROPOSED] ORDER GRANTING, IN PART, MICROSOFT'S MOTION FOR A PARTIAL STAY

Defendant's Counsel are directed to serve this order upon all other parties in this actions.

1   Having considered Defendant Microsoft's Motion for Partial Stay, the supporting

2   and opposing papers, the pleadings and papers on file with the Court, the evidence presented by

3   counsel, oral argument by counsel, and good cause appearing therefor,

4   IT IS HEREBY ORDERED that Microsoft's motion is GRANTED, IN PART, AS

5   FOLLOWS:

6   The parties have selected the following 12 claims for limited <u>Markman</u> claim

7   construction and indefiniteness proceedings:

8   • U.S. Patent No. 6,185,683 – claim 2

9   • U.S. Patent No. 6,253,193 – claims 1, 11, 15, 19

10   • U.S. Patent No. 5,920,861 – claim 58

11   • U.S. Patent No. 5,892,900 – claim 155

12   • U.S. Patent No. 5,982,891 – claim 1

13   • U.S. Patent No. 5,917,912 – claims 8, 35

14   • U.S. Patent No. 6,157,721 – claims 1, 34

15   The Court shall schedule the hearing on Microsoft's anticipated motion for partial

16   summary judgment of indefiniteness (limited to all or some of these 12 claims) to coincide with

17   the <u>Markman</u> hearing on these 12 claims.

18   All proceedings (including all discovery) unrelated to the claim construction and

19   alleged indefiniteness of these 12 claims shall be stayed pending the Court's ruling on these

20   issues.

21   The relatedness of discovery requests to the limited <u>Markman</u> and indefiniteness

22   proceedings shall be construed broadly and both parties are ordered to make every effort to permit

23   discovery, otherwise relevant and discoverable under the Civil Rules, that is colorably related to

24   or likely to assist in developing issues affecting the claim construction and/or indefiniteness of the

25   12 claims selected by the parties. For example, at the hearing counsel represented that they

26   would not object to discovery directed to the use, by either party, of claim terms selected to be

27   construed at the limited Markman hearing, as well as technical documents mentioning those claim

28   terms. However, the failure to object to such discovery <u>shall not</u> be construed as an admission of

1 the admissibility or relevance of that material, nor shall it be considered a waiver of the right to

2 contest its admissibility for any purpose.

3   This partial stay is granted pursuant to the Court's broad powers of case

4 management, including the power to limit discovery to relevant subject matter and to adjust

5 discovery as appropriate to each phase of litigation as set forth by the Federal Circuit in *Vivid*

6 *Technologies, Inc. v. American Science & Engineering, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999),

7 and pursuant to Federal Rules of Civil Procedure 16(b), (c); 26(b); 42(b).

8 Dated: _11—1_, 2002

9

10   The Honorable Saundra Brown Armstrong

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

DECLARATION OF SERVICE VIA ELECTRONIC MAIL AND U.S. MAIL

I am more than eighteen years old and not a party to this action. My place of employment and business address is 1000 Marsh Road, Menlo Park, California 94025.

On November 6, 2002, I served:

ORDER GRANTING, IN PART, MICROSOFT'S MOTION FOR A PARTIAL STAY

By transmitting a copy of the above-listed document(s) in PDF form via electronic mail **Michael H. Page at mhp@kvn.com, Steven H. Morrissett at steven.morrissett@finnegan.com, Stephen E. Taylor at staylor@tcolaw.com and James E. Geringer at james.geringer@klarquist.com** and also by placing true and correct copies of the above documents in an envelope addressed to:

John W. Keker, Esq.
Michael H. Page, Esq.
KEKER & VAN NEST, LLP
710 Sansome Street
San Francisco, California 94111
Tel. No. 415-391-5400
Fax No. 415-397-7188
Email: mhp@kvn.com

Attorneys for Plaintiff INTERTRUST TECHNOLOGIES CORPORATION

Steven H. Morrissett, Esq.
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP
Stanford Research Park
700 Hansen Way
Palo Alto, California 94304-1016
Tel. No. 650-849-6624
Fax No. 650-849-6666
Email: steven.morrissett@finnegan.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

Stephen E. Taylor, Esq.
TAYLOR & CO. LAW OFFICES
1050 Marina Village Parkway, Suite 101
Alameda, CA 94501
Tel. No. 510-865-9401
Fax No. 510-865-9408
Email: staylor@tcolaw.com

Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES
CORPORATION

John D. Vandenberg, Esq.
James E. Geringer, Esq.
KLARQUIST, SPARKMAN, LLP
One World Trade Center
121 S. W. Salmon Street, Suite 1600
Portland, Oregon 97204
Tel. No: 503-226-7391
Fax No: 503-228-9446
Email: james.geringer@klarquist.com

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

and sealing the envelope, affixing adequate first-class postage and depositing it in the U.S. mail at Menlo Park, California.

Executed on November 6, 2002 at Menlo Park, California.

I declare under penalty of perjury that the foregoing is true and correct.

_____
ANNA FREDDIE

ORIGINAL
FILED

NOV 0 6 2002

1 KEKER & VAN NEST, LLP
   JOHN W. KEKER - #49092
2 MICHAEL H. PAGE - #154913
   710 Sansome Street
3 San Francisco, CA 94111-1704
   Telephone: (415) 391-5400
4 Facsimile: (415) 397-7188

5 INTERTRUST TECHNOLOGIES CORPORATION
   DOUGLAS K. DERWIN - #111407
6 MARK SCADINA - #173103
   JEFF MCDOW - #184727
7 4800 Patrick Henry Drive
   Santa Clara, CA 95054
8 Telephone: (408) 855-0100
   Facsimile: (408) 855-0144

9
   Attorneys for Plaintiff and Counter-Defendant
10 INTERTRUST TECHNOLOGIES CORPORATION

R E C E I V E D

NOV - 4 2002

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND

11

12   UNITED STATES DISTRICT COURT

13   NORTHERN DISTRICT OF CALIFORNIA

14

15 INTERTRUST TECHNOLOGIES   Case No. C 01-1640 SBA (MEJ)
   CORPORATION, a Delaware corporation,
16   Consolidated with C 02-0647 SBA
                          Plaintiff,
17   [PROPOSED] FURTHER CASE
                                        MANAGEMENT ORDER
18   v.

19 MICROSOFT CORPORATION, a
   Washington corporation.
20   Plaintiff's C~ ---- ~- directed to serve this
                          Defendant.   order up:. __ .__ ..ries in this action.

21 AND COUNTER ACTION.

22

23

24   On October 31, 2002, this Court conducted a further telephonic Case Management

25 Conference. Pursuant to that conference, the Court ORDERS:

26   SELECTION OF CLAIMS TO BE CONSTRUED

27   The following twelve claims have been selected to be the subject of a "mini-Markman"

28 and "indefiniteness" hearing:

                                    1

Patent No. 6,253,193 B1:   Claims 1, 11, 15 & 19

Patent No. 6,157,721:   Claims 1 & 34

Patent No. 5,917,912:   Claims 8 & 35

Patent No. 5,920,861:   Claim 58

Patent No. 5,982,891:   Claim 1

Patent No. 6,185,683 B1:   Claim 2

Patent No. 5,892,900:   Claim 155

SCHEDULE

The Court adopts the following schedule:

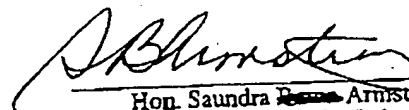| Action To Be Taken	Date
Patent L.R. 4-1 exchange of proposed terms and claim elements for construction for the Twelve Selected InterTrust Patent Claims	11/08/02
Patent L.R. 4-2 exchange of preliminary claim constructions and extrinsic evidence for the Twelve Selected InterTrust Patent Claims	12/20/02
Last day for parties to meet and confer for the purpose of preparing joint claim construction statement for the Twelve Selected InterTrust Patent Claims	1/17/03
Parties to file Patent L.R. 4-3 joint claim construction statement for the Twelve Selected InterTrust Patent Claims	1/31/03
Further Telephonic Case Management Conference (regarding format and length of Markman hearing and briefing)	2/13/03 2:30 p.m.
Completion of claim construction discovery pursuant to Patent L.R. 4-4 for the Twelve Selected InterTrust Patent Claims (other than depositions of declarants)	2/28/03
File and serve opening claim construction brief(s) pursuant to Patent L.R. 4-5(a) for the Twelve Selected InterTrust Patent Claims	3/17/03
File and serve Motion(s) for Partial Summary Judgment (for one or more of the Twelve Selected InterTrust Patent Claims) on issue of indefiniteness under 35 U.S.C. § 112(2)	3/17/03
File and serve opposition brief(s) pursuant to Patent L.R. 4-5(b) for the Twelve Selected InterTrust Patent Claims	4/7/03
File and serve Opposition to any Motion for Partial Summary Judgment (for one or more of the Twelve Selected InterTrust Patent Claims) on issue of indefiniteness under 35 U.S.C. § 112(2)	

2

Action To Be Taken	Date
File and serve reply claim construction brief(s) pursuant to Patent L.R. 4-5(c) for the Twelve Selected InterTrust Patent Claims	4/21/03
File and serve Reply on any Motion for Partial Summary Judgment (for one or more of the Twelve Selected InterTrust Patent Claims) on issue of indefiniteness under 35 U.S.C. § 112(2)	4/21/03
Patent L.R. 4-6 claim construction hearing (and, possibly, technology tutorial) for Twelve Selected InterTrust Patent Claims and Motion for Partial Summary Judgment (for one or more of the Twelve Selected InterTrust Patent Claims) on issue of indefiniteness under 35 U.S.C. § 112(2)	May 12, 29, & 30, 2003
Further Case Management Conference	45 days after Ruling(s)

OTHER MATTERS DISCUSSED

The Court defers consideration of the format of the Markman and/or indefiniteness hearing, and of the length and number of briefs, to the February 13, 2003 Further Case Management Conference. The parties shall address these issues in their Further Case Management Conference Statement.

IT IS SO ORDERED.

DATED: November 5, 2002

_____
Hon. Saundra Brown Armstrong
United States District Judge

[PROPOSED] FURTHER CASE MANAGEMENT ORDER
CASE NO. C 01-1640 SBA (MEJ). CONSOLIDATED WITH C 02-0647 SBA

301151.01

PROOF OF SERVICE

1

2   I am employed in the City and County of San Francisco, State of California in the office of a
    member of the bar of this court at whose direction the following service was made. I am over the
3   age of eighteen years and not a party to the within action. My business address is Keker & Van
    Nest, LLP, 710 Sansome Street, San Francisco, California 94111.
4

5   On November 7, 2002, I served the following document(s):

6   NOTICE OF ENTRY OF FURTHER CASE MANAGEMENT ORDER

7   ☑   by FACSIMILE TRANSMISSION (IKON) AND UNITED STATES MAIL, by placing a true and
        correct copy with IKON Office Solutions, the firm's in-house facsimile transmission center provider, for
        transmission on this date. The transmission was reported as complete and without error. A true and correct
8   copy of same was placed in a sealed envelope addressed as shown below. I am readily familiar with the
        practice of Keker & Van Nest, LLP for collection and processing of correspondence for mailing.
9   According to that practice, items are deposited with the United States Postal Service at San Francisco,
        California on that same day with postage thereon fully prepaid. I am aware that, on motion of the party
10   served, service is presumed invalid if the postal cancellation date or the postage meter date is more than one
        day after the date of deposit for mailing stated in this affidavit.

11

12 Eric L Wesenberg, Esq.   John D. Vandenberg, Esq.
    Mark R. Weinstein, Esq.   James E. Geringer, Esq.
13 Orrick Herrington & Sutcliffe   Kristin L. Cleveland, Esq.
    1000 Marsh Road   Klarquist Sparkman Campbell, et al.
14 Menlo Park, CA 94025   One World Trade Center, Suite 1600
    Telephone: 650/614-7400   121 S.W. Salmon Street
15 Facsimile: 650/614-7401   Portland OR 97204
                                                  Telephone: 503/226-7391
16   Facsimile: 503/228-9446

17

18 I declare under penalty of perjury under the laws of the State of California that the above is true
    and correct.

19
    Executed on November 7, 2002, at San Francisco, California.
20

21

22   NOELLE S. NICHOLS

23

24

25

26

27

28

1

1 | WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
2 | MARK R. WEINSTEIN (State Bar No. 193043)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
3 | 1000 Marsh Road
Menlo Park, CA 94025
4 | Telephone: (650) 614-7400
Facsimile: (650) 614-7401

5

6 | STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
7 | JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
8 | KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
9 | 121 S.W. Salmon Street
Portland, OR 97204
10 | Telephone: (503) 226-7391
Facsimile: (503) 228-9446

11 | Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION
12

13 | UNITED STATES DISTRICT COURT

14 | NORTHERN DISTRICT OF CALIFORNIA

15 | OAKLAND DIVISION

16 | INTERTRUST TECHNOLOGIES
CORPORATION, a Delaware corporation,
17 | Plaintiff,

18 | v.

19 | MICROSOFT CORPORATION, a
Washington corporation,
20 | Defendant.

21 | MICROSOFT CORPORATION, a
Washington corporation,
22
Counterclaimant,
23
v.
24 | INTERTRUST TECHNOLOGIES
CORPORATION, a Delaware corporation,
25
Counterclaim-Defendant.
26

27

28

CASE NO. C 01-1640 SBA (MEJ)

MICROSOFT CORPORATION'S
ANSWER AND COUNTERCLAIMS TO
INTERTRUST'S FOURTH AMENDED
COMPLAINT

DEMAND FOR JURY TRIAL

ORRICK
HERRINGTON
SUTCLIFFE LLP
SILICON VALLEY

Defendant Microsoft Corporation ("Microsoft") answers the Fourth Amended Complaint of InterTrust Technologies Corporation ("InterTrust") as follows:

1.   Microsoft admits that the Fourth Amended Complaint purports to state a cause of action under the patent laws of the United States, 35 United States Code, §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Fourth Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 1 of the Fourth Amended Complaint.

2.   Microsoft admits that the Fourth Amended Complaint purports to state a cause of action over which this Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

3.   Microsoft admits, for purposes of this action only, that venue is proper in this judicial district. Microsoft denies any and all remaining allegations of paragraph 3 of the Fourth Amended Complaint.

4.   On information and belief, Microsoft admits the allegations of paragraph 4 of the Fourth Amended Complaint.

5.   Microsoft admits the allegations of paragraph 5 of the Fourth Amended Complaint.

6.   Microsoft denies any and all allegations of paragraph 6 of the Fourth Amended Complaint, except that it admits, for purposes of this action only, that it transacts business in this judicial district.

7.   Microsoft admits that on its face the title page of U.S. Patent No. 6,185,683 B1 ("the '683 Patent") states that it was issued February 6, 2001, is entitled "Trusted and secure techniques, systems and methods for item delivery and execution," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '683 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 7 of the Fourth Amended Complaint.

1   8.   Microsoft admits that on its face the title page of U.S. Patent No. 6,253,193

2   B1 ("the '193 Patent") states that it was issued June 26, 2001, is entitled "Systems and methods

3   for the secure transaction management and electronic rights protection," and lists "InterTrust

4   Technologies Corporation" as the assignee. Microsoft denies that the '193 Patent was duly and

5   lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 8 of the

6   Fourth Amended Complaint.

7   9.   Microsoft admits that on its face the title page of U.S. Patent No. 5,920,861

8   ("the '861 Patent") states that it was issued July 6, 1999, is entitled "Techniques for defining

9   using and manipulating rights management data structures," and lists "InterTrust Technologies

10 Corp." as the assignee. Microsoft denies that the '861 Patent was duly and lawfully issued.

11 Microsoft further denies any and all remaining allegations of paragraph 9 of the Fourth Amended

12 Complaint.

13   10.   Microsoft admits that on its face the title page of U.S. Patent No. 5,892,900

14 ("the '900 Patent") states that it was issued April 6, 1999, is entitled "Systems and methods for

15 secure transaction management and electronic rights protection," and lists "InterTrust

16 Technologies Corp." as the assignee. Microsoft denies that the '900 Patent was duly and lawfully

17 issued. Microsoft further denies any and all remaining allegations of paragraph 10 of the Fourth

18 Amended Complaint.

19   11.   Microsoft admits that on its face the title page of U.S. Patent No. 5,982,891

20 ("the '891 Patent") states that it was issued November 9, 1999, is entitled "Systems and methods

21 for secure transaction management and electronic rights protection," and lists "InterTrust

22 Technologies Corp." as the assignee. Microsoft denies that the '891 Patent was duly and lawfully

23 issued. Microsoft further denies any and all remaining allegations of paragraph 11 of the Fourth

24 Amended Complaint.

25   12.   Microsoft admits that on its face the title page of U.S. Patent No. 5,917,912

26 ("the '912 Patent") states that it was issued June 29, 1999, is entitled "System and methods for

27 secure transaction management and electronic rights protection," and lists "InterTrust

28 Technologies Corp." as the assignee. Microsoft denies that the '912 Patent was duly and lawfully

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-2-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

1   issued. Microsoft further denies any and all remaining allegations of paragraph 12 of the Fourth

2   Amended Complaint.

3   13.   Microsoft admits that on its face the title page of U.S. Patent No. 6,157,721

4   ("the '721 Patent") states that it was issued December 5, 2000, is entitled "System and methods

5   using cryptography to protect secure computing environments," and lists "InterTrust

6   Technologies Corp." as the assignee. Microsoft denies that the '721 Patent was duly and lawfully

7   issued. Microsoft further denies any and all remaining allegations of paragraph 13 of the Fourth

8   Amended Complaint.

9   14.   Microsoft admits that on its face the title page of U.S. Patent No. 5,915,019

10 ("the '019 Patent") states that it was issued June 22, 1999, is entitled "Systems and methods for

11 secure transaction management and electronic rights protection," and lists "InterTrust

12 Technologies Corp." as the assignee. Microsoft denies that the '019 Patent was duly and lawfully

13 issued. Microsoft further denies any and all remaining allegations of paragraph 14 of the Fourth

14 Amended Complaint.

15   15.   Microsoft admits that on its face the title page of U.S. Patent No. 5,949,876

16 ("the '876 Patent") states that it was issued September 7, 1999, is entitled "Systems and methods

17 for secure transaction management and electronic rights protection," and lists "InterTrust

18 Technologies Corp." as the assignee. Microsoft denies that the '876 Patent was duly and lawfully

19 issued. Microsoft further denies any and all remaining allegations of paragraph 15 of the Fourth

20 Amended Complaint.

21   16.   Microsoft admits that on its face the title page of U.S. Patent No. 6,112,181

22 ("the '181 Patent") states that it was issued August 29, 2000, is entitled "Systems and methods for

23 matching, selecting, narrowcasting, and/or classifying based on rights management and/or other

24 information," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the

25 '181 Patent was duly and lawfully issued. Microsoft further denies any and all remaining

26 allegations of paragraph 16 of the Fourth Amended Complaint.

27   17.   Microsoft admits that on its face the title page of U.S. Patent No. 6,389,402

28 B1 ("the '402 Patent") states that it was issued May 14, 2002, is entitled "Systems and methods

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-3-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

for secure transaction management and electronic rights protection," and lists "InterTrust Technologies Corp." as the assignee. Microsoft denies that the '402 Patent was duly and lawfully issued. Microsoft further denies any and all remaining allegations of paragraph 17 of the Fourth Amended Complaint.

18.   Microsoft repeats and reasserts its responses to paragraphs 1-7 of the Fourth Amended Complaint, as if fully restated herein.

19.   Microsoft admits that the Fourth Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Fourth Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 19 of the Fourth Amended Complaint.

20.   Microsoft denies any and all allegations of paragraph 20 of the Fourth Amended Complaint.

21.   Microsoft denies any and all allegations of paragraph 21 of the Fourth Amended Complaint.

22.   Microsoft denies any and all allegations of paragraph 22 of the Fourth Amended Complaint.

23.   Microsoft denies any and all allegations of paragraph 23 of the Fourth Amended Complaint.

24.   Microsoft denies any and all allegations of paragraph 24 of the Fourth Amended Complaint.

25.   Microsoft repeats and reasserts its responses to paragraphs 1-6 and 8 of the Fourth Amended Complaint, as if fully restated herein.

26.   Microsoft admits that the Fourth Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Fourth Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 26 of the Fourth Amended Complaint.

27.   Microsoft denies any and all allegations of paragraph 27 of the Fourth Amended Complaint.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-4-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

28.   Microsoft denies any and all allegations of paragraph 28 of the Fourth Amended Complaint.

29.   Microsoft denies any and all allegations of paragraph 29 of the Fourth Amended Complaint.

30.   Microsoft denies any and all allegations of paragraph 30 of the Fourth Amended Complaint.

31.   Microsoft denies any and all allegations of paragraph 31 of the Fourth Amended Complaint.

32.   Microsoft repeats and reasserts its responses to paragraphs 1-6 and 9 of the Fourth Amended Complaint, as if fully restated herein.

33.   Microsoft admits that the Fourth Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Fourth Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 33 of the Fourth Amended Complaint.

34.   Microsoft denies any and all allegations of paragraph 34 of the Fourth Amended Complaint.

35.   Microsoft denies any and all allegations of paragraph 35 of the Fourth Amended Complaint.

36.   Microsoft denies any and all allegations of paragraph 36 of the Fourth Amended Complaint.

37.   Microsoft denies any and all allegations of paragraph 37 of the Fourth Amended Complaint.

38.   Microsoft denies any and all allegations of paragraph 38 of the Fourth Amended Complaint.

39.   Microsoft repeats and reasserts its responses to paragraphs 1-6 and 10 of the Fourth Amended Complaint, as if fully restated herein.

40.   Microsoft admits that the Fourth Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-5-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

1   infringes the patents asserted against Microsoft in the Fourth Amended Complaint. Microsoft

2   denies any and all remaining allegations of paragraph 40 of the Fourth Amended Complaint.

3   41.   Microsoft denies any and all allegations of paragraph 41 of the Fourth

4   Amended Complaint.

5   42.   Microsoft denies any and all allegations of paragraph 42 of the Fourth

6   Amended Complaint.

7   43.   Microsoft denies any and all allegations of paragraph 43 of the Fourth

8   Amended Complaint.

9   44.   Microsoft denies any and all allegations of paragraph 44 of the Fourth

10   Amended Complaint.

11   45.   Microsoft denies any and all allegations of paragraph 45 of the Fourth

12   Amended Complaint.

13   46.   Microsoft repeats and reasserts its responses to paragraphs 1-6 and 11 of

14   the Fourth Amended Complaint, as if fully restated herein.

15   47.   Microsoft admits that the Fourth Amended Complaint purports to state a

16   cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now

17   infringes the patents asserted against Microsoft in the Fourth Amended Complaint. Microsoft

18   denies any and all remaining allegations of paragraph 47 of the Fourth Amended Complaint.

19   48.   Microsoft denies any and all allegations of paragraph 48 of the Fourth

20   Amended Complaint.

21   49.   Microsoft denies any and all allegations of paragraph 49 of the Fourth

22   Amended Complaint.

23   50.   Microsoft denies any and all allegations of paragraph 50 of the Fourth

24   Amended Complaint.

25   51.   Microsoft denies any and all allegations of paragraph 51 of the Fourth

26   Amended Complaint.

27   52.   Microsoft denies any and all allegations of paragraph 52 of the Fourth

28   Amended Complaint.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-6-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

53. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 12 of the Fourth Amended Complaint, as if fully restated herein.

54. Microsoft admits that the Fourth Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Fourth Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 54 of the Fourth Amended Complaint.

55. Microsoft denies any and all allegations of paragraph 55 of the Fourth Amended Complaint.

56. Microsoft denies any and all allegations of paragraph 56 of the Fourth Amended Complaint.

57. Microsoft denies any and all allegations of paragraph 57 of the Fourth Amended Complaint.

58. Microsoft denies any and all allegations of paragraph 58 of the Fourth Amended Complaint.

59. Microsoft denies any and all allegations of paragraph 59 of the Fourth Amended Complaint.

60. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 13 of the Fourth Amended Complaint, as if fully restated herein.

61. Microsoft admits that the Fourth Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Fourth Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 61 of the Fourth Amended Complaint.

62. Microsoft denies any and all allegations of paragraph 62 of the Fourth Amended Complaint.

63. Microsoft denies any and all allegations of paragraph 63 of the Fourth Amended Complaint.

64. Microsoft denies any and all allegations of paragraph 64 of the Fourth Amended Complaint.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-7-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

65.   Microsoft denies any and all allegations of paragraph 65 of the Fourth Amended Complaint.

66.   Microsoft denies any and all allegations of paragraph 66 of the Fourth Amended Complaint.

67.   Microsoft repeats and reasserts its responses to paragraphs 1-6 and 14 of the Fourth Amended Complaint, as if fully restated herein.

68.   Microsoft admits that the Fourth Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Fourth Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 68 of the Fourth Amended Complaint.

69.   Microsoft denies any and all allegations of paragraph 69 of the Fourth Amended Complaint.

70.   Microsoft denies any and all allegations of paragraph 70 of the Fourth Amended Complaint.

71.   Microsoft denies any and all allegations of paragraph 71 of the Fourth Amended Complaint.

72.   Microsoft denies any and all allegations of paragraph 72 of the Fourth Amended Complaint.

73.   Microsoft denies any and all allegations of paragraph 73 of the Fourth Amended Complaint.

74.   Microsoft repeats and reasserts its responses to paragraphs 1-6 and 15 of the Fourth Amended Complaint, as if fully restated herein.

75.   Microsoft admits that the Fourth Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Fourth Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 75 of the Fourth Amended Complaint.

76.   Microsoft denies any and all allegations of paragraph 76 of the Fourth Amended Complaint.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-8-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

77. Microsoft denies any and all allegations of paragraph 77 of the Fourth Amended Complaint.

78. Microsoft denies any and all allegations of paragraph 78 of the Fourth Amended Complaint.

79. Microsoft denies any and all allegations of paragraph 79 of the Fourth Amended Complaint.

80. Microsoft denies any and all allegations of paragraph 80 of the Fourth Amended Complaint.

81. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 16 of the Fourth Amended Complaint, as if fully restated herein.

82. Microsoft admits that the Fourth Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft in the Fourth Amended Complaint. Microsoft denies any and all remaining allegations of paragraph 82 of the Fourth Amended Complaint.

83. Microsoft denies any and all allegations of paragraph 83 of the Fourth Amended Complaint.

84. Microsoft denies any and all allegations of paragraph 84 of the Fourth Amended Complaint.

85. Microsoft denies any and all allegations of paragraph 85 of the Fourth Amended Complaint.

86. Microsoft denies any and all allegations of paragraph 86 of the Fourth Amended Complaint.

87. Microsoft denies any and all allegations of paragraph 87 of the Fourth Amended Complaint.

88. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 17 of the Fourth Amended Complaint, as if fully restated herein.

89. Microsoft admits that the Fourth Amended Complaint purports to state a cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-9-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

infringes the patents asserted against Microsoft in the Fourth Amended Complaint. Microsoft

denies any and all remaining allegations of paragraph 89 of the Fourth Amended Complaint.

90. Microsoft denies any and all allegations of paragraph 90 of the Fourth Amended Complaint.

91. Microsoft denies any and all allegations of paragraph 91 of the Fourth Amended Complaint.

92. Microsoft denies any and all allegations of paragraph 92 of the Fourth Amended Complaint.

93. Microsoft denies any and all allegations of paragraph 93 of the Fourth Amended Complaint.

94. Microsoft denies any and all allegations of paragraph 94 of the Fourth Amended Complaint.

AFFIRMATIVE AND OTHER DEFENSES

Further answering the Fourth Amended Complaint, Microsoft asserts the following defenses. Microsoft reserves the right to amend its answer with additional defenses as further information is obtained.

First Defense: Noninfringement of the Asserted Patents

95. Microsoft has not infringed, contributed to the infringement of, or induced the infringement of U.S. Patent No. 6,185,683 B1 ("the '683 Patent"), U.S. Patent No. 6,253,193 B1 ("the '193 Patent"), U.S. Patent No. 5,920,861 ("the '861 Patent"), U.S. Patent No. 5,892,900 ("the '900 Patent"), U.S. Patent No. 5,982,891 ("the '891 Patent"), U.S. Patent No. 5,917,912 ("the '912 Patent"), U.S. Patent No. 6,157,721 ("the '721 Patent"), U.S. Patent No. 5,915,019 ("the '019 Patent"), U.S. Patent No. 5,949,876 ("the '876 Patent"), U.S. Patent No. 6,112,181 ("the '181 Patent"), or U.S. Patent No. 6,389,402 B1 ("the '402 Patent") and is not liable for infringement thereof.

96. Any and all Microsoft products or methods that are accused of infringement have substantial uses that do not infringe and therefore cannot induce or contribute to the infringement of the '683 Patent, the '193 Patent, the '861 Patent, the '900 Patent, the '891

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-10-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

1 Patent, the '912 Patent, the '721 Patent, the '019 Patent, the '876 Patent, the '181 Patent, or the

2 '402 Patent.

Second Defense: Invalidity of the Asserted Patents

4 97.   On information and belief, the '683 Patent, the '193 Patent, the '861

5 Patent, the '900 Patent, the '891 Patent, the '912 Patent, the '721 Patent, the '019 Patent, the '876

6 Patent, the '181 Patent, and the '402 Patent are invalid for failing to comply with the provisions

7 of the Patent Laws, Title 35 U.S.C., including without limitation one or more of 35 U.S.C. §§

8 102, 103 and 112.

Third Defense: Unavailability of Relief

10 98.   On information and belief, Plaintiff has failed to plead and meet the

11 requirements of 35 U.S.C. § 271(b) and (c) and is not entitled to any alleged damages prior to

12 providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '861 Patent, the

13 '900 Patent, the '891 Patent, the '912 Patent, the '721 Patent, the '019 Patent, the '876 Patent, the

14 '181 Patent, or the '402 Patent.

Fourth Defense: Unavailability of Relief

16 99.   On information and belief, Plaintiff has failed to plead and meet the

17 requirements of 35 U.S.C. § 284 for enhanced damages and is not entitled to any damages prior to

18 providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '861 Patent, the

19 '900 Patent, the '891 Patent, the '912 Patent, the '721 Patent, the '019 Patent, the '876 Patent, the

20 '181 Patent, and/or the '402 Patent and any alleged infringement thereof.

Fifth Defense: Unavailability of Relief

22 100.   On information and belief, Plaintiff has failed to plead and meet the

23 requirements of 35 U.S.C. § 287, and has otherwise failed to show that it is entitled to any

24 damages.

Sixth Defense: Prosecution History Estoppel

26 101.   Plaintiff's alleged causes of action for patent infringement are barred under

27 the doctrine of prosecution history estoppel, and Plaintiff is estopped from claiming that the '683

28 Patent, the '193 Patent, the '861 Patent, the '900 Patent, the '891 Patent, the '912 Patent, the '721

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-11-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

Patent, the '019 Patent, the '876 Patent, the '181 Patent, and/or the '402 Patent covers or includes any accused Microsoft product or method.

Seventh Defense: Dedication to the Public

102.   Plaintiff has dedicated to the public all methods, apparatus, and products disclosed in the '683 Patent, the '193 Patent, the '861 Patent, the '900 Patent, the '891 Patent, the '912 Patent, the '721 Patent, the '019 Patent, the '876 Patent, the '181 Patent, and/or the '402 Patent but not literally claimed therein, and is estopped from claiming infringement by any such public domain methods, apparatus, and products.

Eighth Defense: Use/Manufacture By/For United States Government

103.   To the extent that any accused product has been used or manufactured by or for the United States, Plaintiff's claims and demands for relief are barred by 28 U.S.C. § 1498.

Ninth Defense: License

104.   To the extent that any of Plaintiff's allegations of infringement are premised on the alleged use, sale, offer for sale, license or offer of license of products that were manufactured by or for a licensee of InterTrust and/or provided by or to Microsoft by or to a licensee of InterTrust, such allegations are barred pursuant to license.

Tenth Defense: Acquiescence

105.   Plaintiff has acquiesced in at least a substantial part of the Microsoft conduct alleged to infringe.

Eleventh Defense: Laches

106.   Plaintiff's claims for relief are barred, in whole or in part, by the equitable doctrine of laches.

Twelfth Defense: Inequitable Conduct

107.   The '861 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Microsoft's Counterclaim for Declaratory Judgment of Unenforceability of the '861 Patent, set forth below.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-12-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

Thirteenth Defense: Inequitable Conduct

108. The '900 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Microsoft's Counterclaim for Declaratory Judgment of Unenforceability of the '900 Patent, set forth below.

Fourteenth Defense: Inequitable Conduct

109. The '721 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Microsoft's Counterclaim for Declaratory Judgment of Unenforceability of the '721 Patent, set forth below.

Fifteenth Defense: Inequitable Conduct

110. The '181 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Microsoft's Counterclaim for Declaratory Judgment of Unenforceability of the '181 Patent, set forth below.

Sixteenth Defense: Unenforceability

111. The claims of the '891 Patent, the '912 Patent, the '861 Patent, the '683 Patent, the '193 Patent, the '900 Patent, the '721 Patent, the '019 Patent, the '876 Patent, the '181 Patent, and the '402 Patent are unenforceable due to unclean hands, inequitable conduct and misuse and illegal extension of the patent right, including those acts and failures to act set forth in Count XVIII of Microsoft's Counterclaims, set forth below.

Seventeenth Defense: Waiver

112. InterTrust has waived any accusations against Microsoft not made in the InterTrust's Amended Disclosures of Asserted Claims served October 29, 2002, including in particular any "draft" accusations referred to in Court October 22, 2002, that were not included in those Amended Disclosures.

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

COUNTERCLAIMS

COUNT I - DECLARATORY
JUDGMENT OF NONINFRINGEMENT

1.   This action arises under the patent laws of the United States, Title 35 U.S.C. §§ 1, et seq. This Court has subject matter jurisdiction over this counterclaim under 28 U.S.C. §§ 1338, 2201, and 2202.

2.   Microsoft Corporation ("Microsoft") is a Washington corporation with its principal place of business in Redmond, Washington.

3.   On information and belief, Plaintiff /Counterclaim Defendant InterTrust Technologies Corporation ("InterTrust") is a Delaware corporation with its principal place of business in Santa Clara, California.

4.   InterTrust purports to be the owner of U.S. Patent Nos. 6,185,683 B1 ("the '683 Patent"), 6,253,193 B1 ("the '193 Patent"), 5,940,504 ("the '504 Patent"), 5,920,861 ("the '861 Patent"), U.S. Patent No. 5,892,900 ("the '900 Patent"), U.S. Patent No. 5,982,891 ("the '891 Patent"), U.S. Patent No. 5,917,912 ("the '912 Patent"), U.S. Patent No. 6,157,721 ("the '721 Patent"), U.S. Patent No. 5,915,019 ("the '019 Patent"), U.S. Patent No. 5,949,876 ("the '876 Patent"), U.S. Patent No. 6,112,181 ("the '181 Patent"), and U.S. Patent No. 6,389,402 B1 ("the '402 Patent").

5.   InterTrust alleges that Microsoft has infringed the '683 Patent, the '193 Patent, the '861 Patent, the '900 Patent, the '891 Patent, the '912 Patent, the '721 Patent, the '019 Patent, the '876 Patent, the '181 Patent, and the '402 Patent. InterTrust previously alleged that Microsoft has infringed the '504 Patent. InterTrust now concedes that the previously accused Microsoft conduct and products do not infringe any claim of the '504 Patent. No Microsoft product accused in this lawsuit infringes any claim of the '504 Patent.

6.   No Microsoft product has infringed, either directly or indirectly, any claim of the '683 Patent, the '193 Patent, the '504 Patent, the '861 Patent, the '900 Patent, the '891 Patent, the '912 Patent, the '721 Patent, the '019 Patent, the '876 Patent, the '181 Patent, or the '402 Patent, and Microsoft is not liable for infringement thereof.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-14-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

7.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to the infringement or noninfringement of the '683 Patent, the '193 Patent, the '861 Patent, the '900 Patent, the '891 Patent, the '912 Patent, the '721 Patent, the '019 Patent, the '876 Patent, the '181 Patent, and the '402 Patent. If InterTrust does not concede noninfringement of the '504 Patent, then such an actual controversy also exists for the '504 Patent.

COUNT II - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '683 PATENT

8.   Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated here.

9.   The '683 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

10.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '683 Patent are valid or invalid.

COUNT III - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '193 PATENT

11.   Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated here.

12.   The '193 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

13.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '193 Patent are valid or invalid.

COUNT IV - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '504 PATENT

14.   Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated here.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-15-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

15.   The '504 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

16.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '504 Patent are valid or invalid.

COUNT V - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '861 PATENT

17.   Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated here.

18.   The '861 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

19.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '861 Patent are valid or invalid.

COUNT VI - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '900 PATENT

20.   Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated here.

21.   The '900 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

22.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '900 Patent are valid or invalid.

COUNT VII - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '891 PATENT

23.   Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated here.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-16-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

24.   The '891 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

25.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '891 Patent are valid or invalid.

**COUNT VIII - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '912 PATENT**

26.   Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated here.

27.   The '912 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

28.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '912 Patent are valid or invalid.

**COUNT IX - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '721 PATENT**

29.   Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated here.

30.   The '721 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

31.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '721 Patent are valid or invalid.

**COUNT X - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '019 PATENT**

32.   Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated here.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-17-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

33. The '019 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

34. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '019 Patent are valid or invalid.

**COUNT XI - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '876 PATENT**

35. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated here.

36. The '876 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

37. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '876 Patent are valid or invalid.

**COUNT XII - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '181 PATENT**

38. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated here.

39. The '181 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

40. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '181 Patent are valid or invalid.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-18-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

COUNT XIII - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '402 PATENT

41.   Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if fully restated here.

42.   The '402 Patent, and each claim thereof, is invalid for failing to comply with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103, and 112.

43.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '402 Patent are valid or invalid.

COUNT XIV - DECLARATORY JUDGMENT
OF UNENFORCEABILITY OF THE '861 PATENT

44.   Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if fully restated here.

45.   Claims 1-129 of the '861 Patent application (SN 08/805,804), and claims 1-101 of the '861 Patent, were not and are not entitled to the benefit of any application filing date prior to February 25, 1997, under 35 U.S.C. § 120 or otherwise.

46.   On information and belief, an article entitled "DigiBox: A Self-Protecting Container for Information Commerce" (hereinafter "the Sibert article") was published in the United States in July 1995. A copy of the Sibert article has been produced bearing bates numbers MSI022935-MSI022947.

47.   "Exhibit A" refers to the document attached as Exhibit A to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint (namely, a reprint of an article entitled "DigiBox: A Self-Protecting Container for Information Commerce"). On information and belief, the content of pages 2-14 of Exhibit A was presented at a public conference in the United States in July 1995.

48.   "Exhibit B" refers to the document attached as Exhibit B to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint (namely, a copy of a

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-19-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

page from an International Application published under the Patent Cooperation Treaty (PCT), bearing International Publication Number WO 96/27155 hereinafter (hereafter "the WO 96/27155 (PCT) publication")).

49.   On information and belief, the WO 96/27155 (PCT) publication has, at all times since its filing date, been owned and controlled by InterTrust or its predecessors in interest.

50.   The WO 96/27155 (PCT) publication was published on September 6, 1996.

51.   United States Patent No. 5,910,987 ("the '987 Patent") issued on June 8, 1999, from a continuation of an application filed on February 13, 1995.

52.   The Sibert article is prior art to claims 1-129 of the '861 Patent application (SN 08/805,804).

53.   The Sibert article is prior art to claims 1-101 of the '861 Patent under 35 U.S.C. § 102(b).

54.   The WO 96/27155 (PCT) publication is prior art to claims 1-129 of the '861 Patent application (SN 08/805,804).

55.   The WO 96/27155 (PCT) publication is prior art to claims 1-101 of the '861 Patent under 35 U.S.C. § 102(a).

56.   The '987 Patent is prior art to claims 29-129 of the '861 Patent application (SN 08/805,804).

57.   The '987 Patent is prior art to claims 1-101 of the '861 Patent, under 35 U.S.C. § 102(e).

58.   The Sibert article was material to the patentability of claim 1 of the '861 Patent application (SN 08/805,804).

59.   The Sibert article was material to the patentability of claims 2-129 of the '861 Patent application (SN 08/805,804).

60.   The WO 96/27155 (PCT) publication was material to the patentability of claim 1 of the '861 Patent application (SN 08/805,804).

61.   The WO 96/27155 (PCT) publication was material to the patentability of claims 2-129 of the '861 Patent application (SN 08/805,804).

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-20-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

1   62.   The '987 Patent was material to the patentability of claims 29-129 of the

2 '861 Patent application (SN 08/805,804).

3   63.   One or more of the '861 Patent applicants knew, while the '861 Patent

4 application (SN 08/805,804) was pending, of the July 1995 publication of the Sibert article.

5   64.   On information and belief, one or more of the '861 Patent applicants knew,

6 while the '861 Patent application (SN 08/805,804) was pending, of the September 1996

7 publication of the WO 96/27155 (PCT) publication.

8   65.   On information and belief, one or more of the '861 Patent applicants knew,

9 while the '861 Patent application (SN 08/805,804) was pending, of the June 8, 1999 issuance of

10 the '987 Patent.

11   66.   On information and belief, one or more of the attorneys who prosecuted or

12 assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application

13 was pending, of the July 1995 publication of the Sibert article.

14   67.   One or more of the attorneys who prosecuted or assisted in prosecuting the

15 '861 Patent application (SN 08/805,804) knew, while that application was pending, of the

16 September 1996 publication of the WO 96/27155 (PCT) publication.

17   68.   One or more of the attorneys who prosecuted or assisted in prosecuting the

18 '861 Patent application (SN 08/805,804) knew, while that application was pending, of the June 8,

19 1999 issuance of the '987 Patent.

20   69.   The applicants for the '861 Patent did not cite the Sibert article to the

21 Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804).

22   70.   The applicants for the '861 Patent did not cite the WO 96/27155 (PCT)

23 publication to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application

24 (SN 08/805,804).

25   71.   The applicants for the '861 Patent did not cite the '987 Patent to the Patent

26 Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804).

27

28

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-21-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

72. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the Sibert article.

73. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the WO 96/27155 (PCT) publication.

74. The applicants for the '861 Patent did not cite to the Patent Office as prior art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having the same or substantially the same disclosure as the '987 Patent.

75. The Sibert article is not merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

76. The WO 96/27155 (PCT) publication is not merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

77. The '987 Patent is not merely cumulative over any reference cited as prior art during the prosecution of the '861 Patent application (SN 08/805,804).

78. On information and belief, one or more of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the Sibert article disclosed an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

79. InterTrust contends that none of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the Sibert article discloses an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

80. On information and belief, one or more of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the WO 96/27155 (PCT) publication disclosed an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

81. InterTrust contends that none of the '861 Patent applicants believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the WO 96/27155

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-22-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

1 (PCT) publication discloses an embodiment of claim 1 of the '861 Patent application (SN

2 08/805,804).

3   82.   On information and belief, one or more of the '861 Patent applicants

4 believed, while the '861 Patent application (SN 08/805,804) was pending, that the Sibert article

5 was material to the patentability of claims 1-129 of the '861 Patent application (SN 08/805,804),

6 but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

7   83.   On information and belief, one or more of the '861 Patent applicants

8 believed, while the '861 Patent application (SN 08/805,804) was pending, that the WO 96/27155

9 (PCT) publication was material to the patentability of claims 1-129 of the '861 Patent application

10 (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the

11 Patent Office.

12   84.   On information and belief, one or more of the '861 Patent applicants

13 believed, while the '861 Patent application (SN 08/805,804) was pending, that the '987 Patent

14 was material to the patentability of claims 29-129 of the '861 Patent application (SN 08/805,804),

15 but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

16   85.   The '861 Patent is unenforceable due to the inequitable conduct of the '861

17 Patent applicants and/or agents before the Patent and Trademark Office in connection with the

18 '861 Patent application (SN 08/805,804).

19   86.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202,

20 exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to

21 whether the claims of the '861 Patent are enforceable.

22 <div align="center">**COUNT XV - DECLARATORY JUDGMENT**
OF UNENFORCEABILITY OF THE '900 PATENT</div>

23

24   87.   Microsoft repeats and realleges paragraphs 1-5 and 46-47 of its

25 Counterclaims, as if fully restated here.

26   88.   The application and issued claims of the '900 Patent were not and are not

27 entitled to the benefit of any application filing date prior to August 30, 1996, under 35 U.S.C. §

28 120 or otherwise.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-23-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

89.   The Sibert article is prior art to the application and issued claims of the '900 Patent under 35 U.S.C. § 102(b).

90.   The Sibert article was material to the patentability of application and issued claims of the '900 Patent, including, for example, issued claims 86 and 182.

91.   One or more of the '900 Patent applicants knew of the July 1995 publication of the Sibert article while the '900 Patent application (SN 08/706,206) was pending.

92.   On information and belief, one or more of the attorneys who prosecuted or assisted in the prosecution of the '900 Patent application (SN 08/706,206) knew of the July 1995 publication of the Sibert article while the '900 Patent application was pending.

93.   The applicants for the '900 Patent did not cite the Sibert article to the Patent Office as prior art to any claims of the '900 Patent application (SN 08/706,206).

94.   The applicants for the '900 Patent did not cite to the Patent Office as prior art to any claims of the '900 Patent application (SN 08/706,206) any reference having the same or substantially the same disclosure as the Sibert article.

95.   The Sibert article is not merely cumulative over any reference cited as prior art during the prosecution of the '900 Patent application (SN 08/706,206).

96.   On information and belief, one or more of the '900 Patent applicants believed, during pendency of claim 1 of the '900 Patent application (SN 08/706,206), that the Sibert article disclosed an embodiment of claim 1 of the '900 Patent application (SN 08/706,206).

97.   On information and belief, one or more of the '900 Patent applicants believed, while the '900 Patent application (SN 08/706,206) was pending, that the Sibert article was material to the patentability of various claims of the '900 Patent application (SN 08/706,206), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

98.   The '900 Patent is unenforceable due to the inequitable conduct of the '900 Patent applicants and/or agents before the Patent and Trademark Office in connection with the '900 Patent application (SN 08/706,206).

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-24-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

99.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '900 Patent are enforceable.

COUNT XVI - DECLARATORY JUDGMENT
OF UNENFORCEABILITY OF THE '721 PATENT

100.   Microsoft repeats and realleges paragraphs 1-5 and 51 of its Counterclaims, as if fully restated herein.

101.   Claims 1-43 of the '721 Patent application (SN 08/689,754), and claims 1-41 of the '721 Patent, were not and are not entitled to the benefit of any application filing date prior to August 12, 1996, under 35 U.S.C. § 120 or otherwise.

102.   The '987 Patent is prior art to claims 1-8, 10-29, and 31-43 of the '721 Patent application (SN 08/689,754).

103.   The '987 Patent is prior art to claims 1-41 of the '721 Patent under 35 U.S.C. § 102(e).

104.   The '987 Patent was material to the patentability of claims 1-8, 10-29, and 31-43 of the '721 Patent application (SN 08/689,754).

105.   One or more of the '721 Patent applicants knew, while the '721 Patent application (SN 08/689,754) was pending, of the '987 Patent.

106.   On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '721 Patent application (SN 08/689,754) knew, while that application was pending, of the '987 Patent.

107.   The applicants for the '721 Patent did not cite the '987 Patent to the Patent Office as prior art to any of claims 1-43 of the '721 Patent application (SN 08/689,754).

108.   The applicants for the '721 Patent did not cite to the Patent Office as prior art to any of claims 1-43 of the '721 Patent application (SN 08/689,754) any reference having the same or substantially the same disclosure as the '987 Patent.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-25-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

109.   The '987 Patent is not merely cumulative over any reference cited as prior art during the prosecution of the '721 Patent application (SN 08/689,754).

110.   On information and belief, one or more of the '721 Patent applicants believed, while the '721 Patent application (SN 08/689,754) was pending, that the '987 Patent was material to the patentability of one or more of claims 1-8, 10-29, and 31-43 of the '721 Patent application (SN 08/689,754), but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

111.   The applicants for the '721 Patent knew of, but did not cite to the Patent Office as prior art to any of the claims of the '721 Patent application (SN 08/689,754), printed publications regarding the use of digital signatures with Java.

112.   On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '721 Patent application knew, while that application was pending, of printed publications describing the use of digital signatures with Java, but did not cite those publications to the Patent Office.

113.   On information and belief, one or more of the '721 Patent applicants knew of General Magic's Telescript, (hereinafter "Telescript"), while the '721 Patent application (SN 08/689,754) was pending.

114.   On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '721 Patent application knew, while that application was pending, of Telescript.

115.   On information and belief, one or more of the '721 Patent applicants knew, while the '721 Patent application (SN 08/689,754) was pending, of work done by Doug Tygar and Bennett Yee regarding "Strongbox," (hereinafter "Strongbox").

116.   On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '721 Patent application knew, while that application was pending, of work done by Doug Tygar and Bennett Yee regarding "Strongbox."

117. Strongbox, Telescript, and publications regarding the use of digital signatures with Java are each material prior art to the '721 Patent.

118. On information and belief, InterTrust's failure to disclose Strongbox, Telescript, and/or publications regarding the use of digital signatures with Java was made with deceptive intent.

119. The '721 Patent is unenforceable due to the inequitable conduct of the '721 Patent applicants and/or agents before the Patent and Trademark Office in connection with the '721 Patent application (SN 08/689,754).

120. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '721 Patent are enforceable.

COUNT XVII – DECLARATORY JUDGMENT OF UNENFORCEABILITY OF THE '181 PATENT

121. Microsoft repeats and realleges paragraphs 1-5 and 46-51 of its Counterclaims, as if fully restated herein.

122. The claims of the '181 Patent were not and are not entitled to the benefit of any application filing date prior to November 6, 1997, under 35 U.S.C. § 120 or otherwise.

123. The '987 Patent is prior art to the claims of the '181 Patent.

124. The '987 Patent is prior art to each claim of the '181 Patent under 35 U.S.C. § 102(e).

125. The '987 Patent was material to the patentability of one or more claims of the '181 Patent application (SN 08/965,185).

126. One or more of the '181 Patent applicants knew, while the '181 Patent application (SN 08/965,185) was pending, of the '987 Patent.

127. On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '181 Patent application knew, while that application was pending, of the '987 Patent.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-27-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

128. The applicants for the '181 Patent did not cite the '987 Patent to the Patent Office as prior art to any of the claims of the '181 Patent application (SN 08/965,185).

129. The applicants for the '181 Patent did not cite to the Patent Office as prior art to any of the claims of the '181 Patent application any reference having the same or substantially the same disclosure as the '987 Patent.

130. The '987 Patent is not merely cumulative over any reference cited as prior art during the prosecution of the '181 Patent application.

131. On information and belief, one or more of the '181 Patent applicants believed, while the '181 Patent application (SN 08/965,185) was pending, that the '987 Patent was material to the patentability of one or more of claims of the '181 Patent application (SN 08/689,754).

132. On information and belief, one or more of the '181 Patent applicants, with deceptive intent, failed to disclose the '987 Patent as prior art to the Patent Office during the prosecution of the '181 Patent application (SN 08/965,185).

133. The Sibert article is prior art to the application and issued claims of the '181 Patent under 35 U.S.C. § 102(b).

134. The Sibert article was material to the patentability of one or more claims sought by InterTrust in the course of the '181 Patent application.

135. The Sibert article was material to the patentability of one or more claims of the '181 Patent.

136. One or more of the '181 Patent applicants knew of the July 1995 publication of the Sibert article while the '181 Patent application (SN 08/965,185) was pending.

137. On information and belief, one or more of the attorneys who prosecuted or assisted in the prosecution of the '181 Patent application (SN 08/965,185) knew of the July 1995 publication of the Sibert article while the '181 Patent application was pending.

138. The applicants for the '181 Patent did not cite the Sibert article to the Patent Office as prior art to any claims of the '181 Patent application (SN 08/965,185).

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-28-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

1   139.   The applicants for the '181 Patent did not cite to the Patent Office as prior

2   art to any claims of the '181 Patent application (SN 08/965,185) any reference having the same or

3   substantially the same disclosure as the Sibert article.

4   140.   The Sibert article is not merely cumulative over any reference cited as prior

5   art during the prosecution of the '181 Patent application (SN 08/965,185).

6   141.   On information and belief, one or more of the '181 Patent applicants

7   believed, while the '181 Patent application (SN 08/965,185) was pending, that the Sibert article

8   was material to the patentability of one or more claims of the '181 Patent application (SN

9   08/965,185).

10   142.   On information and belief, one or more of the '181 Patent applicants, with

11   deceptive intent, failed to disclose the Sibert article as prior art to the Patent Office during the

12   prosecution of the '181 Patent application (SN 08/965,185).

13   143.   The WO 96/27155 (PCT) publication is prior art to one or more claims of

14   the '181 Patent application.

15   144.   The WO 96/27155 (PCT) publication is prior art to the claims of the '181

16   Patent under 35 U.S.C. § 102(a).

17   145.   The WO 96/27155 (PCT) publication is prior art to the claims of the '181

18   Patent under 35 U.S.C. § 102(b).

19   146.   The WO 96/27155 (PCT) publication was material to the patentability of

20   claim 1 of the '181 Patent application (SN 08/965,185).

21   147.   The WO 96/27155 (PCT) publication was material to the patentability of

22   one or more claims of the '181 Patent application (SN 08/965,185).

23   148.   On information and belief, one or more of the '181 Patent applicants knew,

24   while the '181 Patent application (SN 08/965,185) was pending, of the September 1996

25   publication of the WO 96/27155 (PCT) publication.

26   149.   One or more of the attorneys who prosecuted or assisted in prosecuting the

27   '181 Patent application (SN 08/965,185) knew, while that application was pending, of the

28   September 1996 publication of the WO 96/27155 (PCT) publication.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-29-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

150. The applicants for the '181 Patent did not cite the WO 96/27155 (PCT) publication to the Patent Office as prior art to any of the claims of the '181 Patent application (SN 08/965,185).

151. The applicants for the '181 Patent did not cite to the Patent Office as prior art to any of the claims of the '181 Patent application (SN 08/965,185) any reference having the same or substantially the same disclosure as the WO 96/27155 (PCT) publication.

152. On information and belief, one or more of the '181 Patent applicants believed, while the '181 Patent application (SN 08/965,185) was pending, that the WO 96/27155 (PCT) publication was material to the patentability of one or more claims of the '181 Patent application (SN 08/965,185).

153. On information and belief, one or more of the '181 Patent applicants, with deceptive intent, failed to disclose the WO 96/27155 (PCT) publication as prior art to the Patent Office during the prosecution of the '181 Patent application (SN 08/965,185).

154. The '900 Patent (U.S. Pat. No. 5,892,900) is prior art to the '181 Patent.

155. The '900 Patent is prior art to one or more claims of the '181 Patent under 35 U.S.C. § 102(e).

156. The '900 Patent was material to the patentability of one or more claims of the '181 Patent application (SN 08/965,185).

157. One or more of the '181 Patent applicants knew, while the '181 Patent application (SN 08/965,185) was pending, of the '900 Patent.

158. On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '181 Patent application knew, while that application was pending, of the '900 Patent.

159. The applicants for the '181 Patent did not cite the '900 Patent to the Patent Office as prior art to any of the claims of the '181 Patent application (SN 08/965,185).

160. The applicants for the '181 Patent did not cite to the Patent Office as prior art to any of the claims of the '181 Patent application any reference having the same or substantially the same disclosure as the '900 Patent.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-30-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE No. C 01-1640 SBA

161. The '900 Patent is not merely cumulative over any reference cited as prior art during the prosecution of the '181 Patent application.

162. On information and belief, one or more of the '181 Patent applicants believed, while the '181 Patent application (SN 08/965,185) was pending, that the '900 Patent was material to the patentability of one or more of claims of the '181 Patent application (SN 08/689,754).

163. On information and belief, one or more of the '181 Patent applicants, with deceptive intent, failed to disclose the '900 Patent as prior art to the Patent Office during the prosecution of the '181 Patent application (SN 08/965,185).

164. The '721 Patent (U.S. Pat. No. 6,157,721) is prior art to the '181 Patent.

165. The '721 Patent is prior art to one or more claims of the '181 Patent under 35 U.S.C. § 102(e).

166. The '721 Patent was material to the patentability of one or more claims of the '181 Patent application (SN 08/965,185).

167. One or more of the '181 Patent applicants knew, while the '181 Patent application (SN 08/965,185) was pending, of the '721 Patent.

168. On information and belief, one or more of the attorneys who prosecuted or assisted in prosecuting the '181 Patent application knew, while that application was pending, of the '721 Patent.

169. The applicants for the '181 Patent did not cite the '721 Patent to the Patent Office as prior art to any of the claims of the '181 Patent application (SN 08/965,185).

170. The applicants for the '181 Patent did not cite to the Patent Office as prior art to any of the claims of the '181 Patent application any reference having the same or substantially the same disclosure as the '721 Patent.

171. The '721 Patent is not merely cumulative over any reference cited as prior art during the prosecution of the '181 Patent application.

172. On information and belief, one or more of the '181 Patent applicants believed, while the '181 Patent application (SN 08/965,185) was pending, that the '721 Patent

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-31-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

was material to the patentability of one or more of claims of the '181 Patent application (SN 08/689,754).

173. On information and belief, one or more of the '181 Patent applicants, with deceptive intent, failed to disclose the '721 Patent as prior art to the Patent Office during the prosecution of the '181 Patent application (SN 08/965,185).

174. The '181 Patent is unenforceable due to the inequitable conduct of the '181 Patent applicants and/or agents before the Patent and Trademark Office in connection with the '181 Patent application (SN 08/965,185).

175. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202, exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to whether the claims of the '181 Patent are enforceable.

COUNT XVIII - DECLARATORY JUDGMENT OF UNENFORCEABILITY

176. Microsoft repeats and realleges the preceding paragraphs of its Counterclaims, as if fully restated here.

177. The '891 Patent, the '912 Patent, the '683 Patent, the '193 Patent, the '861 Patent, the '900 Patent, the '721 Patent, the '019 Patent, the '876 Patent, the '181 Patent, and the '402 Patent are referred to as the "Count XVIII Patents."

178. In prosecuting, marketing, and enforcing the Count XVIII Patents, InterTrust has engaged in a pattern of obfuscation as to the scope of the patents, the prior art to the patents, and the alleged "inventions" of the patents.

179. InterTrust has accused non-infringing products of infringement in this case.

180. InterTrust has accused non-secure products with infringement in this case.

181. InterTrust has buried Patent Office Examiners with a collection of more than 400 references, many of which were not related to the particular claims in issue.

182. InterTrust has buried the Examiners with hundreds of thousands of pages of redundant, verbose, unclear text, effectively prohibiting a real comparison of the alleged "invention" to the prior art.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-32-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

183. This pattern of intentional conduct constitutes an abuse of the patent system, unclean hands, misuse and illegal extension of the patent right, rendering the Count XVIII patents unenforceable, as well as invalid under 35 U.S.C. § 112.

184. InterTrust contends that it cannot readily determine whether or not it has ever practiced the claims it asserts in this case, as InterTrust has interpreted those claims in its PLR 3-1 Statements.

185. InterTrust contends that it cannot determine, with reasonable effort, whether or not it has ever used its Commerce or Rights/System software to practice any of the claims InterTrust asserts in this case, as InterTrust has interpreted those claims in its PLR 3-1 Statements.

186. As InterTrust has interpreted the claims it asserts in this case in its PLR 3-1 Statements, InterTrust does not know if it has ever practiced the subject matter of the patent claims it asserts in this case.

187. No InterTrust officer has a non-privileged opinion or belief as to whether InterTrust has ever practiced the subject matter of any of the patent claims it asserts in this case.

188. InterTrust contends that it cannot readily determine whether or not any entity not a party to this case has ever practiced the claims that InterTrust asserts in this case, as InterTrust has interpreted those claims in this case.

189. InterTrust contends that it cannot readily determine whether or not any of the references cited in the patents it asserts in this case describes any invention that InterTrust asserts is disclosed in any patent it asserts in this case.

190. No InterTrust officer has a non-privileged opinion or belief as to whether Sony (whether Sony Corporation, Sony Corporation of America, and/or Sony Music Entertainment Inc.), IBM, Adobe, AT&T, or Real Networks has ever practiced the subject matter of any of the patent claims that InterTrust asserts in this case.

191. No InterTrust officer has a non-privileged opinion or belief as to whether Sony (whether Sony Corporation, Sony Corporation of America, and/or Sony Music

1 Entertainment Inc.), IBM, Adobe, AT&T, or Real Networks has ever practiced a noninfringing

2 alternative to any of the patent claims that InterTrust asserts in this case.

3   192.   No InterTrust officer has a non-privileged opinion or belief as to whether

4 the U.S. government has ever practiced the subject matter of any of the patent claims that

5 InterTrust asserts in this case.

6   193.   InterTrust has never built the "Virtual Distribution Environment" referred

7 to at column 2 lines 22-35 of the '193 Patent.

8   194.   No Microsoft product accused in this case is a "Virtual Distribution

9 Environment" as referred to at column 2 lines 22-35 of the '193 Patent.

10   195.   As InterTrust's PLR 3-1 Statements have interpreted the '683 Patent claims

11 asserted in this case, one or more of those claims reads upon references that InterTrust cited to the

12 Patent Office during prosecution of the '683 Patent.

13   196.   As InterTrust's PLR 3-1 Statements have interpreted the '683 Patent claims

14 asserted in this case, InterTrust cannot distinguish those claims from the subject matter disclosed

15 in the specification of U.S. Patent 5,715,403.

16   197.   As InterTrust's PLR 3-1 Statements have interpreted the '683 Patent claims

17 asserted in this case, InterTrust cannot distinguish those claims from the subject matter disclosed

18 in the cited reference WO 93/01550.

19   198.   As InterTrust's PLR 3-1 Statements have interpreted the '193 Patent claims

20 asserted in this case, one or more of those claims reads upon the subject matter disclosed in the

21 specification of U.S. Patent 5,638,443.

22   199.   An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202,

23 exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to

24 whether the claims of the '891 Patent, the '912 Patent, the '683 Patent, the '193 Patent, the '861

25 Patent, and the '900 Patent, the '721 Patent, the '019 Patent, the '876 Patent, the '181 Patent, and

26 the '402 Patent are enforceable.

27

28

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-34-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

COUNT XIX - INFRINGEMENT
OF U.S. PATENT NO. 6,049,671

200. Microsoft repeats and realleges paragraphs 2-3 of its Counterclaims, as if fully restated here.

201. This Court has exclusive subject matter jurisdiction over Microsoft's cause of action for patent infringement under Title 28, United States Code, Sections 1331 and 1338, and under the patent laws of the United States, Title 35 of the United States Code.

202. U.S. Patent No. 6,049,671 ("the '671 Patent") issued to Microsoft Corporation as the assignee of Benjamin W. Slivka and Jeffrey S. Webber on April 11, 2000.

203. A true copy of the '671 Patent is attached as Exhibit C to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint, and is incorporated herein by reference.

204. Microsoft owns all right, title and interest in the '671 Patent.

205. InterTrust has had actual notice of the '671 Patent.

206. InterTrust has infringed one or more claims of the '671 Patent, in violation of at least 35 U.S.C. § 271(a, b, c).

207. InterTrust's infringement of the '671 Patent has caused and will continue to cause Microsoft damage, including irreparable harm for which it has no adequate remedy at law.

COUNT XX - INFRINGEMENT
OF U.S. PATENT NO. 6,256,668

208. Microsoft repeats and realleges paragraphs 2-3 and 201 of its Counterclaims, as if fully restated here.

209. U.S. Patent No. 6,256,668 B1 ("the '668 Patent") issued to Microsoft Corporation as the assignee of Benjamin W. Slivka and Jeffrey S. Webber on July 3, 2001.

210. A true copy of the '668 Patent is attached as Exhibit D to Microsoft's counterclaims filed in response to InterTrust's Second Amended Complaint, and is incorporated herein by reference.

211. Microsoft owns all right, title and interest in the '668 Patent.

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-35-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

212. InterTrust has had actual notice of the '668 Patent.

213. InterTrust has infringed one or more claims of the '668 Patent, in violation of at least 35 U.S.C. § 271(a, b, c).

214. InterTrust's infringement of the '668 Patent has caused and will continue to cause Microsoft damage, including irreparable harm for which it has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays for the following relief:

A.   The Court enter judgment against InterTrust, and dismiss with prejudice, any and all claims of the Fourth Amended Complaint;

B.   The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '683 Patent;

C.   The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '193 Patent;

D.   The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '504 Patent;

E.   The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '861 Patent;

F.   The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '900 Patent;

G.   The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '891 Patent;

H.   The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '912 Patent;

I.   The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '721 Patent;

J.   The Court enter judgment declaring that Microsoft has not infringed, contributed to infringement of, or induced infringement of the '019 Patent;

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-36-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

1   K.   The Court enter judgment declaring that Microsoft has not infringed,

2 contributed to infringement of, or induced infringement of the '876 Patent;

3   L.   The Court enter judgment declaring that Microsoft has not infringed,

4 contributed to infringement of, or induced infringement of the '181 Patent;

5   M.   The Court enter judgment declaring that Microsoft has not infringed,

6 contributed to infringement of, or induced infringement of the '402 Patent;

7   N.   The Court enter judgment declaring that the '683 Patent is invalid;

8   O.   The Court enter judgment declaring that the '193 Patent is invalid;

9   P.   The Court enter judgment declaring that the '504 Patent is invalid;

10   Q.   The Court enter judgment declaring that the '861 Patent is invalid;

11   R.   The Court enter judgment declaring that the '900 Patent is invalid;

12   S.   The Court enter judgment declaring that the '891 Patent is invalid;

13   T.   The Court enter judgment declaring that the '912 Patent is invalid;

14   U.   The Court enter judgment declaring that the '721 Patent is invalid;

15   V.   The Court enter judgment declaring that the '019 Patent is invalid;

16   W.   The Court enter judgment declaring that the '876 Patent is invalid;

17   X.   The Court enter judgment declaring that the '181 Patent is invalid;

18   Y.   The Court enter judgment declaring that the '402 Patent is invalid;

19   Z.   The Court enter judgment declaring that the '861 Patent, the '900 Patent,

20 the '721 Patent, and the '181 Patent are each unenforceable due to inequitable conduct;

21   AA.   The Court enter judgment declaring that each of the '891 Patent, the '912

22 Patent, the '683 Patent, the '193 Patent, the '861 Patent, the '900 Patent, the '721 Patent, the '019

23 Patent, the '876 Patent, the '181 Patent, and the '402 Patent is unenforceable due to an abuse of

24 the patent system, unclean hands, and misuse and illegal extension of the patent right;

25   BB.   The Court enter judgment that InterTrust has infringed the '671 Patent;

26   CC.   The Court enter judgment that InterTrust has infringed the '668 Patent;

27

28

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

DD. The Court enter a permanent injunction prohibiting InterTrust, its officers, agents, servants, employees, and all persons in active concert or participation with any of them from infringing the '671 and '668 Patents;

EE. The Court award damages and attorney fees against InterTrust pursuant to the provisions of 35 U.S.C §§ 284 and 285.

FF. The Court award to Microsoft pre-judgment interest and the costs of this action.

GG. The Court award to Microsoft its reasonable costs and attorneys' fees; and

HH. The Court grant to Microsoft such other and further relief as may be deemed just and appropriate.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Defendant Microsoft Corporation demands a trial by jury.

DATED: November 7, 2002

By:_____
WILLIAM L. ANTHONY
ERIC L. WESENBERG
SAM O'ROURKE
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650-614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391

Attorneys for Defendant
Microsoft Corporation

Of Counsel:
T. Andrew Culbert, Esq.
MICROSOFT CORPORATION
One Microsoft Way, Building 8
Redmond, WA 98052-6399
Phone: 425-882-8080

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

-38-

MICROSOFT CORPORATION'S ANSWER AND
COUNTERCLAIMS TO INTERTRUST'S FOURTH AMENDED
COMPLAINT: CASE NO. C 01-1640 SBA

InterTrust's Rule 4-1 Proposed Terms and Claim Elements for Construction

Component Assembly (912.8, 913.35)[1]

Control (193.1, 193.11, 193.15, 193.19, 891.1)

Executable programming/executable (912.8, 912.35, 721.34)

Load module (912.8, 721.1)

Metadata (861.58)

Processing environment (912.35, 900.155, 721.34)

Protected processing environment (721.34)

Record (912.8, 912.35)

Rendering (193.11, 193.15, 193.19)

Rule (861.58, 683.2)

Secure/securely/security (912.8, 912.35, 861.58, 193.1, 193.11, 193.15, 891.1, 683.2, 721.1, 721.34)

Secure container (913.35, 861.58, 683.2)

Tamper/tampering (900.155, 721.1, 721.34)

User controls (683.2)

---

[1] Location of claim terms is indicated in the form [xxx.y], where xxx= the last three digits of the patent number, and y= the claim number.

1 WILLIAM L. ANTHONY (State Bar No. 106908)
   ERIC L. WESENBERG (State Bar No. 139696)
2 MARK R. WEINSTEIN (State Bar No. 193043)
3 ORRICK, HERRINGTON & SUTCLIFFE, LLP
   1000 Marsh Road
4 Menlo Park, CA 94025
   Telephone: (650) 614-7400
5 Facsimile: (650) 614-7401

6 STEVEN ALEXANDER (admitted *Pro Hac Vice*)
7 KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
   JAMES E. GERINGER (admitted *Pro Hac Vice*)
8 JOHN D. VANDENBERG
   KLARQUIST SPARKMAN, LLP
9 One World Trade Center, Suite 1600
   121 S.W. Salmon Street
10 Portland, OR 97204
11 Telephone: (503) 226-7391
   Facsimile: (503) 228-9446

12
   Attorneys for Defendant and Counterclaimant,
13 MICROSOFT CORPORATION

14   UNITED STATES DISTRICT COURT

15   NORTHERN DISTRICT OF CALIFORNIA

16   OAKLAND DIVISION

17 | INTERTRUST TECHNOLOGIES   CASE NO. C01-1640 SBA
   | CORPORATION, a Delaware corporation,
18 |
   | Plaintiff,
19 | MICROSOFT CORPORATION'S
   | v.   PATENT LOCAL RULE 4-1(a)
20 | MICROSOFT CORPORATION, a   STATEMENT (LIMITED TO "MINI-
   | Washington corporation,   MARKMAN" CLAIMS)
21 |
   | Defendant.
22 | MICROSOFT CORPORATION, a
   | Washington corporation,
23 |
   | Counterclaimant,
24 |
   | v.
25 | INTERTRUST TECHNOLOGIES
   | CORPORATION, a Delaware corporation,
26 |
   | Counter Claim-Defendant.
27

28

Pursuant to Patent Local Rule 4-1(a), Microsoft submits below the claim terms, phrases, and clauses of the twelve selected "Mini-Markman" patent claims that Microsoft presently submits, subject to discussions with InterTrust, should be construed by the Court, in addition to construing each claim as a whole.

Set forth in Section A, below, is a list of individual claim terms that Microsoft presently submits, subject to discussions with InterTrust, should be construed by the Court. Individual claim terms should be construed wherever they are found in these twelve claims.

Set forth in Section B, below, are the phrases and clauses that Microsoft presently submits, subject to discussions with InterTrust, should be construed by the Court. The claim phrases and clauses that Microsoft presently submits, subject to discussions with InterTrust, should be governed by 35 U.S.C. § 112(6), are identified in Section B by double underlining.

Many of these claim terms, phrases and clauses are indefinite and otherwise improper under 35 U.S.C. § 112(2), and Microsoft reserves all rights to assert those defects as to each of these claim terms, phrases and clauses.

The grouping of individual claim terms below is for convenience only and does not imply any particular connection, or lack of connection, between any terms.

A.   **Individual Claim Terms**

- a digital file, digital file
- access, accessed, access to, accessing
- addressing
- allowing, allows
- applying . . . in combination
- arrangement
- aspect
- associated with
- authentication
- authorization information, authorized, not authorized
- budget control, budget

1	• can be
2	• capacity
	• clearinghouse
3	• compares, comparison
4	• component assembly
	• contain, contained, containing
5	• control (n.), controls (n.)
6	• controlling, control (v.)
	• copied file
7	• copy, copied, copying
8	• copy control
	• creating, creation
9	• data item
10	• derive, derives
11	• descriptive data structure
	• designating
12	• device class
13	• digital signature, digitally signing
	• entity, entity's control
14	• environment
15	• executable programming, executable
	• execution space, execution space identifier
16	• generating
17	• govern, governed, governed item, governing
	• halting
18	• host processing environment
19	• identifier, identify, identifying
20	• including
	• information previously stored
21	• integrity programming
22	• key
	• load module
23	• machine check programming
24	• metadata information
	• opening secure containers
25	• operating environment, said operating environment
26	• organization, organization information, organize
27	• portion
	• prevents
28	• processing environment

- protected processing environment
- protecting
- record
- required
- resource processed
- rule
- secure
- secure container, secure containers
- secure container governed item
- secure container rule
- secure database
- secure execution space
- secure memory, memory
- secure operating environment, said operating environment
- securely applying
- securely assembling
- securely processing
- securely receiving, securely receiving ... a control
- security
- security level, level of security
- specific information, specified information
- tamper resistance
- tamper resistant barrier
- tamper resistant software
- tampering
- use
- validity
- virtual distribution environment

B.   Claim Phrases and Clauses

'193:1

- receiving a digital file including music
- a budget specifying the number of copies which can be made of said digital file
- controlling the copies made of said digital file
- determining whether said digital file may be copied and stored on a second device based on at least said copy control
- if said copy control allows at least a portion of said digital file to be copied and stored on a second device
- copying at least a portion of said digital file

1 • transferring at least a portion of said digital file to a second device

2 • storing said digital file

'193:11

4 • receiving a digital file

• determining whether said digital file may be copied and stored on a second device based on
5 said first control

6 • identifying said second device

• whether said first control allows transfer of said copied file to said second device

7 • said determination based at least in part on the features present at the device

8 • if said first control allows at least a portion of said digital file to be copied and stored on a
second device

9 • copying at least a portion of said digital file

10 • transferring at least a portion of said digital file to a second device

• storing said digital file

'193:15

12 • receiving a digital file

13 • an authentication step comprising:

14 • accessing at least one identifier associated with a first device or with a user of said first device

• determining whether said identifier is associated with a device and/or user authorized to store
15 said digital file

16 • storing said digital file in a first secure memory of said first device, but only if said device
and/or user is so authorized, but not proceeding with said storing if said device and/or user is
17 not authorized

18 • storing information associated with said digital file in a secure database stored on said first
device, said information including at least one control

19 • determining whether said digital file may be copied and stored on a second device based on
said at least one control

20 • if said at least one control allows at least a portion of said digital file to be copied and stored
on a second device,
21

• copying at least a portion of said digital file

22 • transferring at least a portion of said digital file to a second device

23 • storing said digital file

'193:19

25 • receiving a digital file at a first device

• establishing communication between said first device and a clearinghouse located at a
26 location remote from said first device

27 • using said authorization information to gain access to or make at least one use of said first
digital file

28 • including using said key to decrypt at least a portion of said first digital file

1 • receiving a first control from said clearinghouse at said first device

2 • storing said first digital file in a memory of said first device

3 • using said first control to determine whether said first digital file may be copied and stored on a second device

4 • if said first control allows at least a portion of said first digital file to be copied and stored on a second device

5 • copying at least a portion of said first digital file

6 • transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output

7 • storing said first digital file portion

'683:2

9 • user controls

10 • the first secure container having been received from a second apparatus

   • an aspect of access to or use of

11 • the first secure container rule having been received from a third apparatus different from said second apparatus

12 • hardware or software used for receiving and opening secure containers

13 • said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers

14 • protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus

15

16 • hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container

17

18 • hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.

'721:1

20 • digitally signing a first load module with a first digital signature designating the first load module for use by a first device class

21 • digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class

22

23

24 • distributing the first load module for use by at least one device in the first device class

   • distributing the second load module for use by at least one device in the second device class

25

'721:34

26 • arrangement within the first tamper resistant barrier

27 • prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level

28

'861:58

- creating a first secure container
- including or addressing . . . organization information . . . desired organization . . . and metadata information at least in part specifying at least one step required or desired in creation of said first secure container
- at least in part determine specific information required to be included in said first secure container contents
- rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents

'891:1

- resource processed in a secure operating environment at a first appliance
- securely receiving a first entity's control at said first appliance
- securely receiving a second entity's control at said first appliance
- securely processing a data item at said first appliance, using at least one resource
- securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item

'900:155

- first host processing environment comprising
- said mass storage storing tamper resistant software
- designed to be loaded into said main memory and executed by said central processing unit
- said tamper resistant software comprising: . . . one or more storage locations storing said information
- derives information from one or more aspects of said host processing environment,
- one or more storage locations storing said information
- information previously stored in said one or more storage locations
- generates an indication based on the result of said comparison
- programming which takes one or more actions based on the state of said indication
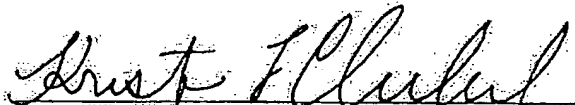- at least temporarily halting further processing

'912:8

- identifying at least one aspect of an execution space
- required for use and/or execution of the load module
- said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security
- checking said record for validity prior to performing said executing step

1

2 • received in a secure container

• said component assembly allowing access to or use of specified information

3 • said first component assembly specified by said first record

4

5 Dated: November 8, 2002

6

7 By: _Krist J Cleveland_

8 WILLIAM L. ANTHONY
ERIC L. WESENBERG

9 MARK R. WEINSTEIN
ORRICK HERRINGTON & SUTCLIFFE, LLP

10 1000 Marsh Road
Menlo Park, CA 94025

11 Telephone: (650) 614-7400

12

STEVEN ALEXANDER

13 KRISTIN L. CLEVELAND
JAMES E. GERINGER

14 JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP

15 One World Trade Center, Suite 1600
121 S.W. Salmon Street

16 Portland, OR 97204
Telephone: (503) 226-7391

17

18 Attorneys for Defendant

19 MICROSOFT CORPORATION

20 Of Counsel:

21 T. Andrew Culbert, Esq.
One Microsoft Way

22 Building 8
Redmond, WA 98052-6399

23 Phone: 425-882-8080

24

25

26

27

28

MICROSOFT CORPORATION'S PATENT LOCAL
RULE 4-1(a) STATEMENT, CASE No. C 01-1640
-8-   SBA

DECLARATION OF SERVICE BY E-MAIL AND FIRST CLASS MAIL

I am more than eighteen years old and not a party to this action. My place of employment and business address is 121 S.W. Salmon St., Suite 1600, Portland, OR 97204.

On November 8, 2002, I served on counsel for InterTrust Technologies Corporation:

MICROSOFT CORPORATION'S PATENT LOCAL RULE 4-1(a) STATEMENT by e-mail delivery and by placing true copies of these papers in envelopes addressed to:

Michael H. Page, Esq. John W. Keker, Esq. Jon B. Streeter, Esq. KEKER & VAN NEST, LLP 710 Sansome Street San Francisco, CA 94111 Phone: 415-391-5400 Fax: 415-397-7188 E-mail: mhp@kvn.com	Stephen E. Taylor, Esq. Taylor & Co. Law Offices 1050 Marina Village Parkway Suite 101 Alameda, CA 94501 Phone: 510-865-9401 Fax: 510-865-9408 Email: staylor@tcolaw.com
Steven H. Morrissett, Esq. Finnegan Henderson Farabow Garrett & Dunner Stanford Research Park 700 Hansen Way Palo Alto CA 94304-1016 steven.morrissett@finnegan.com	

and sealing each envelope, affixing adequate first-class postage and depositing it in the U.S. mail at Portland, Oregon.

I declare under penalty of perjury that the foregoing is true and correct. Executed on November 8, 2002, at Portland, Oregon.

_____
(SIGNATURE)

_____
(PRINT NAME)

1 KEKER & VAN NEST, LLP
   JOHN W. KEKER - #49092
2 MICHAEL H. PAGE - #154913
   710 Sansome Street
3 San Francisco, CA 94111-1704
   Telephone: (415) 391-5400
4 Facsimile: (415) 397-7188

5 INTERTRUST TECHNOLOGIES CORPORATION
   DOUGLAS K. DERWIN - #111407
6 MARK SCADINA - #173103
   JEFF MCDOW - #184727
7 4800 Patrick Henry Drive
   Santa Clara, CA 95054
8 Telephone: (408) 855-0100
   Facsimile: (408) 855-0144

9
   Attorneys for Plaintiff and Counter-Defendant
10 INTERTRUST TECHNOLOGIES CORPORATION

11

12   UNITED STATES DISTRICT COURT

13   NORTHERN DISTRICT OF CALIFORNIA

14

15 INTERTRUST TECHNOLOGIES   Case No. C 01-1640 SBA (MEJ)
    CORPORATION, a Delaware corporation,
16   Consolidated with C 02-0647 SBA
                              Plaintiff,
17   INTERTRUST'S PATENT LOCAL RULE
        v.   4-2 PRELIMINARY CLAIM
18   CONSTRUCTIONS AND
    MICROSOFT CORPORATION, a   IDENTIFICATION OF EVIDENCE
19 Washington corporation,

20   Defendant.

21
    AND COUNTER ACTION.
22

23

24 I. Pat.L.R. 4-2(a) Preliminary Claim Constructions

25   The following constitute InterTrust's proposed definitions for claim terms identified in

26 the parties' Rule 4-1 disclosures. InterTrust reserves the right to modify these definitions in light

27 of definitions, evidence or arguments propounded by Microsoft.

28   Capitalized terms occurring in definitions represent separately-defined terms and should

                                            1

1 be given the same meaning as in the separate definition.

2 The designation of a definition as "normal English" means that InterTrust believes the

3 defined term should have its normal English meaning, with no definition being necessary.

4 Submission of a definition in such cases does not constitute a waiver of InterTrust's right to

5 contend that no such definition is necessary.

6 These terms are defined for the claims specified in the definition. InterTrust reserves the

7 right to assert that these terms should be interpreted differently in contexts other than those

8 specified.

9 Reference citations are to "extrinsic evidence" listed in Section II of this document.

10 Unless otherwise noted, the references constitute dictionaries and the citations are to definitions

11 of the designated terms in such dictionaries.

12 **A. Individual Claim Terms.**

13 **Access.** (193.15, 193.19, 912.8, 912.35, 861.58, 683.2, 721.34)[1]

14 To obtain something so it can be used.

15 References: 1, 2, 6.

16 **Addressing (861.58)**

17 Referring to a location where information is stored.

18 Reference: 3.

19 **Allowing, allows (912.35, 193.1, 193.11, 193.15, 193.19)**

20 Normal English: permitting, permits; letting happen, lets happen.

21 Reference: 4.

22 **Applying in combination (683.2)**

23 Using more than one Rule to Govern a Secure Container Governed Item.

24 **Arrangement (721.34)**

25 Normal English: a collection of things that have been arranged. In context, the
   term can apply to an organization of hardware and/or software and/or data.
26

27 Reference: 4.

28 _____
[1] Patent and Claim numbers are denoted herein in the format "xxx.yy", where "xxx" is the last
   three digits of the patent number and "YY" is the claim number.

2

INTERTRUST'S PATENT LOCAL RULE 4-2 PRELIMINARY CLAIM CONSTRUCTIONS AND
IDENTIFICATION OF EVIDENCE
CASE NO. C 01-1640 SBA (MEJ), CONSOLIDATED WITH C 02-0647 SBA

303750.01

Aspect (900.155, 912.8, 861.58, 683.2)

Feature, element, property or state.

Associated With (912.8, 193.1, 193.11, 193.15, 683.2)

Having a relationship with.

Authentication (193.15)

In context, Identifying (e.g., a person, device, organization, document, file, etc.). Includes uniquely identifying or identifying as a member of a group.

Authorization Information/Authorize/Not Authorize (193.15, 193.19)

Authorize:

Normal English: permit.

References: 4.

Authorization Information:

In context: Information (e.g., a key) received if an action is Authorized. See Specific Information for the definition of Information.

Budget (193.1)

Information specifying a limitation on usage. See Specific Information for the definition of Information.

Reference: 4.

Budget control (193.1)

The term is explicitly defined in the claim as a Control "including a budget specifying the number of copies which can be made of said digital file."

Can be (193.1)

Normal English: the specified act is able or authorized to be carried out. In context, this means the number of copies allowed to be made.

Reference: 4.

Capacity (683.2)

Normal English: "ability," or "capability."

Reference: 4.

Clearinghouse (193.19)

A provider of financial and/or administrative services for a number of users; or an entity responsible for the collection, maintenance, and/or distribution of materials,

3

INTERTRUST'S PATENT LOCAL RULE 4-2 PRELIMINARY CLAIM CONSTRUCTIONS AND
IDENTIFICATION OF EVIDENCE
CASE NO. C 01-1640 SBA (MEJ), CONSOLIDATED WITH C 02-0647 SBA

303750.01

1   information, licenses, etc.

2   **Compares/Comparison (900.155)**

3   Normal English:

4   Compares: examines for the purpose of noting similarities and differences.

5   Reference: 4.

6   Comparison: the act of comparing.

7   Reference: 4.

8   **Component Assembly (912.8, 912.35)**

9   Components are code and/or data elements that are independently deliverable. A
         Component Assembly is two or more components associated together.
10   Component Assemblies are executed to perform operating system or applications
         tasks.

11   **Contained/Contain/Containing (683.2, 912.8, 912.35)**

12

13   Normal English: to have within or to hold. In the context of an element
         contained within a data structure (e.g., a secure container), the contained element
         may be either directly within the container or the container may hold a reference
14   indicating where the element may be found.

15   Reference: 4.

16   **Control (n) (193.1, 193.11, 193.15, 193.19, 891.1)**

17   Information and/or programming Governing operations on or use of Resources
         (e.g., content) including (a) permitted, required or prevented operations, (b) the
18   nature or extent of such operations or (c) the consequences of such operations.

19   **Control (v)/Controlling (861.58, 193.1)**

20   Normal English: to exercise authoritative or dominating influence over; direct.

21   Reference: 4.

22   **Copied file (193.11)**

23   A Digital File that has been Copied.

24   **Copy, copied, copying (193.1, 193.11, 193.15, 193.19)**

25   Reproduce, reproduced, reproducing. The reproduction may incorporate all of the
         original item, or only some of it, and may involve some changes to the item as
26   long as the essential nature of the content remains unchanged.

27   References: 1, 4, 6.

28

303750.01

Copy control (193.1)

A Control used to determine whether a Digital File may be Copied and the Copied Digital File stored on a second device.

Creating/Creation (861.58)

Normal English: Creating means producing; Creation means the act of creating.

Reference: 4.

Data item (891.1)

A unit of digital information.

References: 2, 3.

Derive/Derives (900.155)

Normal English: obtain, receive or arrive at through a process of reasoning or deduction. In the context of computer operations, the "process of reasoning or deduction" constitutes operations carried out by the computer.

Reference: 4.

Descriptive Data Structure (861.58)

Machine-readable description of the layout and/or contents of a rights management data structure (e.g., a Secure Container).

Designating (721.1)

Normal English: indicating, specifying, pointing out or characterizing.

Reference: 4.

Device Class (721.1)

A group of devices which share at least one attribute.

Digital File (193.1, 193.11, 193.15, 193.19)

A named collection of digital information.

Reference: 3 (definition of "file").

Digitally signing/digital signature (721.1)

Digital signature: A digital value, verifiable with a Key, that can be used to determine the source and/or integrity of a signed item (e.g., a file, program, etc.).

Digitally signing is the process of creating a digital signature.

303750.01

Entity/Entity's control (891.1)

Entity: A person or organization.

Entity's Control: Control belonging to or coming from an Entity.

Environment (912.35, 900.155, 891.1, 683.2, 721.34)

Capabilities available to a program running on a computer or other device or to the user of a computer or other device. Depending on the context, the environment may be in a single device (e.g., a personal computer) or may be spread among multiple devices (e.g., a network).

References: 6.

Executable Programming/Executable (912.8, 912.35, 721.34)

A computer program that can be run, directly or through interpretation.

Reference: 3.

Execution space (912.8)

Resource which can be used for execution of a program or process.

Execution space identifier (912.8)

Information Identifying an Execution Space. See Specific Information for definition of Information.

Generates/Generating (900.155, 861.58)

Normal English: creates/creating or produces/producing.

Reference: 4.

Govern/Governed/Governed Item (891.1, 683.2)

To Govern: to control an item or operation in accordance with criteria established by the holder of one or more rights relating to the item or operation or a party authorized to establish such criteria.

Governed Item: an item that is Governed.

Reference: 4.

Halting (900.155)

Normal English: suspending.

Reference: 4.

Host Processing Environment (900.155)

This term is explicitly defined in the claim and therefore needs no additional

6

303750.01

definition. It consists of those elements listed in the claim.

Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: a Protected Processing Environment incorporating software-based Security.

Identifier (193.15, 912.8)

Information used to Identify something or someone (e.g., a password).

Identify/identifying (193.11, 912.8, 912.35, 861.58)

Normal English: To establish/establishing the identity of or to ascertain/ascertaining the origin, nature, or definitive characteristics of.

Reference: 4.

Including (912.8, 912.35, 900.155, 861.58, 193.1, 193.11, 193.15, 193.19, 891.1, 683.2)

Normal English: depending on the context, this means containing as a secondary or subordinate element, or considering with or placing into a group, class, or total.

Reference: 4.

Information previously stored (900.155)

Normal English: Information stored at an earlier time. See Specific Information for the definition of Information.

Integrity programming (900.155)

This term is fully defined in the claim, which specifies the steps the integrity programming must perform. Integrity programming is programming that performs the recited steps. The term therefore needs no additional definition.

Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: programming that checks the integrity of a Host Processing Environment.

Key (193.19)

Information used to encrypt, decrypt, sign or verify other information.

Load Module (912.8, 721.1)

An Executable unit of code designed to be loaded into memory and executed, plus associated data.

References: 3.

Machine Check Programming (900.155)

Programming that checks a host processing environment and derives information from an Aspect of the host processing environment.

7

303750.01

Metadata Information (861.58)

> Information about information. Metadata Information may describe the attributes of a rights management data structure as well as processes used to create and/or use it.

Opening secure containers (683.2)

> Providing Access to the contents of a Secure Container (e.g., by decrypting the contents, if the contents are encrypted).

Operating environment (891.1)

> Environment in which programs function.

> References: 6.

Organize, organization, organization information (861.58)

> In the context of organization of a Secure Container, these terms refer to contents required or desired (including Information used to categorize these contents); or Information used to specify a particular location for content. See Specific Information for the definition of Information.

Portion (193.1, 193.11, 193.15, 193.19, 912.8, 912.35, 861.58)

> Normal English: a part of a whole. The presence of a "portion" does not exclude the presence of the whole (e.g., storage of an entire file necessarily includes storage of any portions into which that file may be subdivided).

> Reference: 4.

Prevents (721.34)

> Normal English: keeps from happening.

> Reference: 4.

Processing Environment (912.35, 900.155, 721.34, 683.2)

> Processing: manipulating data.

> Reference: 3.

> Processing Environment: An Environment used for Processing. A Processing Environment may be made up of one device or of more than one device linked together.

Protected Processing Environment (683.2, 721.34)

> Processing Environment in which processing and/or data is at least in part protected from Tampering. The level of protection can vary, depending on the threat.

Protecting (683.2)

> Normal English: keeping from being damaged, attacked, stolen or injured.

> Reference: 4.

Record (912.8, 912.35)

> Collection of related items of data treated as a unit.

> References: 1.

Rendering (193.11, 193.15, 193,19)

> Playing content through an audio output (e.g., speakers) or displaying content on a video output (e.g., a screen).

Required (912.8, 861.58)

> Normal English: a thing that is required is a thing that is obligatory or demanded.

> Reference: 4.

Resource processed (891.1)

> Resource: computer software, computer hardware, data, data structure or information.

> Resource processed: a Resource subject to being Processed, i.e., computer software, data, data structure or information. See Processing Environment for a definition of Processed.

Rule (861.58, 683.2)

> See Control.

Secure (193.1, 193.11, 193.15, 912.35, 861.58, 891.1, 683.2, 721.34)

> One or more mechanisms are employed to prevent, detect or discourage misuse of or interference with information or processes. Such mechanisms may include concealment, Tamper Resistance, Authentication and access control.
> Concealment means that it is difficult to read information (for example, programs may be encrypted). Tamper Resistance and Authentication are separately defined. Access control means that Access to information or processes is limited on the basis of authorization. Security is not absolute, but is designed to be sufficient for a particular purpose.

> Reference: 6.

Secure Container (912.35, 861.58, 683.2)

> Container: Digital File Containing linked and/or embedded items.

> Reference: 3, 5.

Secure Container: A Container that is Secure.

Secure container governed item (683.2)

Information and/or programming Contained in a Secure Container and Governed by an associated Secure Container Rule.

Secure container rule (683.2)

Rule that at least in part Governs a Secure Container Governed Item.

Secure Database (193.1, 193.11, 193.15)

Database: an organized collection of information.

References: 2.

Database that is Secure.

Secure Execution Space (721.34)

Execution Space that is Secure.

Secure Memory/Memory (193.1, 193.11, 193.15)

Memory: a component of a computer or other device where information can be stored and retrieved.

References: 3, 4.

Secure Memory: Memory in which Information is handled in a Secure manner. See Specific Information for the definition of Information.

Secure Operating Environment (891.1)

An Operating Environment that is Secure.

Securely Applying (891.1)

Requiring that one or more Controls be complied with before content may be used. The operation of requiring that the Control(s) be complied with must be carried out in a Secure manner.

Securely Assembling (912.8, 912.35)

Associating two or more Components together to form a Component Assembly, in a Secure manner. See Component Assembly for the definition of Component.

Securely Processing (891.1)

Processing occurring in a Secure manner. See Processing Environment for the definition of Processing.

10

Securely Receiving (891.1)

Receiving has its normal English meaning: acquiring or getting.

Reference: 4.

Securely Receiving means receipt occurring in a Secure manner.

Security (721.1, 721.34)

Relating to being Secure.

Security Level/Level of Security (721.1; 721.34, 912.8)

Information that can be used to determine how Secure something is (e.g., a device, Tamper Resistant Barrier or Execution Space).

Specified information/specific information (912.35, 861.58)

Normal English meaning:

Specific: explicitly set forth or definite.

Reference: 4.

To specify: to state explicitly or in detail.

Reference: 4.

Information: nonaccidental signal(s) or character(s) used in a computer or communication system. Information includes programs and also includes data.

Reference: 4.

Tamper/Tampering (683.2, 721.1, 721.34, 900.155)

To Use (including observe), alter or interfere with in an unauthorized manner.

Reference: 8.

Tamper Resistant/Tamper Resistance (721.1, 721.34, 900.155)

~~Making Tampering more difficult,~~ and/or allowing detection of Tampering.

Tamper Resistant Barrier (721.34)

Hardware or software that provides Tamper Resistance.

Tamper Resistant Software (900.155)

Software designed to make it more difficult to Tamper with the software.

References: 7, 8.

11

303750.01

Use (912.8, 912.35, 861.58, 193.19, 891.1, 683.2, 721.1)

> Normal English: to put into service or apply for a purpose, to employ. Reference: 4.

User controls (683.2)

> Hardware feature of an apparatus allowing a user to operate the apparatus (e.g., a keyboard).

Validity (912.8)

> A property of something (e.g., a Record) indicating that it is appropriate for use.

Virtual Distribution Environment (900.155)

> This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements.

> Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: secure, distributed electronic transaction management and rights protection system for controlling the distribution and/or other usage of electronically provided and/or stored information.

Claim Phrases and Clauses

193.1

Receiving a digital file including music (193.1)

> See Receiving a digital file (193.11). This phrase is interpreted the same, except that the file includes music.

Budget specifying the number of copies which can be made of said digital file (193.1)

> Normal English, incorporating the separately defined terms: a Budget stating the number of Copies that Can Be made of the Digital File referred to earlier in the claim.

Controlling the copies made of said digital file (193.1)

> The nature of this operation is further defined in later claim elements. In context, the Copy Control determines the conditions under which a Digital File may be Copied and the Copied File stored on a second device.

Determining whether said digital file may be copied and stored on a second device based on at least said copy control (193.1)

> Normal English, incorporating the separately defined terms: Using the Copy Control in deciding whether the Digital File referred to earlier in the claim may be Copied and the Copied Digital File stored on a second device.

If said copy control allows at least a portion of said digital file to be copied and stored on a second device (193.1)

        Normal English: a "yes" result is received in the step Determining whether said digital file may be copied and stored on a second device based on at least said copy control (193.1).

Copying at least a portion of said digital file (193.1, 193.11, 193.15, 193.19)

        Normal English, incorporating the separately defined terms: Copying at least a Portion of the Digital File referred to earlier in the claim.

Transferring at least a portion of said digital file to a second device (193.1, 193.11, 193.15, 193.19)

        Normal English, incorporating the separately defined terms: at least a Portion of the Copied Digital File is sent to a second device.

Storing said digital file (193.1, 193.11, 193.15)

        Normal English: that which was transferred in the transferring step is stored.

193.11

Receiving a digital file (193.1, 193.11, 193.15, 193.19)

        Normal English, incorporating the separately defined term: a Digital File is obtained.

        This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term:

        Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.

Determining whether said digital file may be copied and stored on a second device based on said first control (193.11)

        Normal English, incorporating the separately defined terms: Using the Control to decide whether the Digital File may be Copied and the Copied Digital File stored on the second device.

Identifying said second device (193.11)

        Normal English, incorporating the separately defined term: the second device is Identified.

13

INTERTRUST'S PATENT LOCAL RULE 4-2 PRELIMINARY CLAIM CONSTRUCTIONS AND IDENTIFICATION OF EVIDENCE
CASE NO. C 01-1640 SBA (MEJ), CONSOLIDATED WITH C 02-0647 SBA

303750.01

1   Whether said first control allows transfer of said copied file to said second device
     (193.11)

2   Normal English, incorporating the separately defined terms: Using the first
3   Control to decide if the Copied Digital File may be sent to the second device.

4   Said determination based at least in part on the features present at the device
     (193.11)

5   Normal English: the decision referred to earlier in the claim is based at least in
6   part on characteristics of the second device.

7   If said first control allows at least a portion of said digital file to be copied and
     stored on a second device (193.11)

8   See If said copy control allows at least a portion of said digital file to be copied
9   and stored on a second device (193.1). The definitions are the same.

10   Copying at least a portion of said digital file (193.1, 193.11, 193.15, 193.19)

11   See Copying at least a portion of said digital file (193.1). The definitions are the
          same.

12   Transferring at least a portion of said digital file to a second device (193.1, 193.11,
13   193.15, 193.19)

14   See Transferring at least a portion of said digital file to a second device (193.1).
          The definitions are the same.

15   Storing said digital file (193.1, 193.11, 193.15)

16   See Storing said digital file (193.1). The definitions are the same.

17   193.15

18   Receiving a digital file (193.1, 193.11, 193.15, 193.19

19   See Receiving a digital file (193.11). The definitions are the same.

20   An authentication step comprising (193.15)

21   Normal English, incorporating the separately defined term: a step involving
22   Authentication.

23   Accessing at least one identifier associated with a first device or with a user of said
     first device (193.15)

24   Normal English, incorporating the separately defined terms: Accessing an
25   Identifier Associated With a device or a user of the device.

26   Determining whether said identifier is associated with a device and/or user
     authorized to store said digital file (193.15)

27   Normal English, incorporating the separately defined terms: deciding whether the
28   Identifier is Associated With a device or user with authority to store the Digital

303750.01

1   File.

2   Storing said digital file in a first secure memory of said first device, but only if said
device and/or user is so authorized, but not proceeding with said storing if said device
3   and/or user is not authorized (193.15)

4   Normal English, incorporating the separately defined terms: this step proceeds or
               does not proceed based on the preceding determining step. If this step proceeds,
5   the Digital File is stored in a Secure Memory of the first device.

6   Storing information associated with said digital file in a secure database stored on
said first device, said information including at least one control (193.15)

7

8   Normal English, incorporating the separately defined terms: storing a Control
               Associated With the Digital File in a Secure Database stored at the first device.

9   Determining whether said digital file may be copied and stored on a second device
based on said at least one control (193.15)

10

11   See Determining whether said digital file may be copied and stored on a second
               device based on at least said copy control (193.1). The definitions are the same.

12   If said at least one control allows at least a portion of said digital file to be copied
and stored on a second device (193.15)

13

14   See If said first control allows at least a portion of said digital file to be copied
               and stored on a second device (193.11). The definitions are the same.

15   Copying at least a portion of said digital file (193.1, 193.11, 193.15, 193.19)

16   See Copying at least a portion of said digital file (193.1). The definitions are the
               same.

17

18   Transferring at least a portion of said digital file to a second device (193.1, 193.11,
193.15, 193.19)

19   See Transferring at least a portion of said digital file to a second device (193.1)
               The definitions are the same.

20

21   Storing said digital file (193.1, 193.11, 193.15)

22   See Storing said digital file (193.1) The definitions are the same.

23   193.19

24   Receiving a digital file at a first device (193.19)

25   See Receiving a digital file (193.11). The definitions are the same.

26   Establishing communication between said first device and a clearinghouse located at
a location remote from said first device (193.19)

27   Normal English, incorporating the separately defined term: sending information
               from the first device to the Clearinghouse and/or the first device receiving
28   information from the Clearinghouse.

15

303750.01

This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term:

Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.

Using said authorization information to gain access to or make at least one use of said first digital file (193.19)

Normal English, incorporating the separately defined terms: the Authorization Information is used in a process of Accessing or Using the Digital File.

Including using said key to decrypt at least a portion of said first digital file (193.19)

Normal English, incorporating the separately defined terms: this step further describes the "using said authorization information" step, and requires that the earlier step include using the Key in a process of decrypting of at least a Portion of the Digital File.

Receiving a first control from said clearinghouse at said first device (193.19)

Normal English, incorporating the separately defined terms: the first device acquires or gets a Control from the Clearinghouse.

This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term:

Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.

Storing said first digital file in a memory of said first device (193.19)

Normal English, incorporating the separately defined terms: the Digital File is stored at the first device.

Using said first control to determine whether said first digital file may be copied and stored on a second device (193.19)

See Determining whether said digital file may be copied and stored on a second device based on at least said copy control (193.1). The definitions are the same.

16

303750.01

1   If said first control allows at least a portion of said first digital file to be copied and
stored on a second device (193.19)

2

3   See If said first control allows at least a portion of said digital file to be copied
           and stored on a second device (193.11). The definitions are the same.

4   Copying at least a portion of said first digital file (193.1, 193.11, 193.15, 193.19)

5   See Copying at least a portion of said digital file (193.1). The definitions are the
           same.

6

7   Transferring at least a portion of said first digital file to a second device including a
memory and an audio and/or video output (193.19)

8   See Transferring at least a portion of said digital file to a second device (193.1).
           The definitions are the same, except that the second device has an audio or video
9   output or both (e.g., a speaker, a screen, etc.).

10   Storing said first digital file portion (193.19)

11   Normal English, incorporating the separately defined terms: the Digital File
           Portion is stored.

12

       721.1

13

       Digitally signing a first load module with a first digital signature designating the
14   first load module for use by a first device class (721.1)

15   Normal English, incorporating the separately defined terms: generating a Digital
           Signature for the first Load Module, the Digital Signature Designating that the
16   first Load Module is for use by a first Device Class.

17   Digitally signing a second load module with a second digital signature different from
       the first digital signature, the second digital signature designating the second load module
18   for use by a second device class having at least one of tamper resistance and security level
       different from the at least one of tamper resistance and security level of the first device
19   class (721.1)

20   Normal English, incorporating the separately defined terms: generating a Digital
           Signature for the second Load Module, the Digital Signature Designating that the
21   second Load Module is for use by a second Device Class. This element further
           requires that the second Device Class have a different Tamper Resistance or
22   Security Level than the first Device Class.

23   Distributing the first load module for use by at least one device in the first device
       class (721.1)

24

25   Normal English, incorporating the separately defined terms: distributing the first
           Load Module so that it can be used by a device in the first Device Class.

26   Distributing the second load module for use by at least one device in the second
       device class (721.1)

27

28   Normal English, incorporating the separately defined terms: distributing the
           second Load Module so that it can be used by a device in the second Device

17

1 Class.

2 721.34 ,

3 **Arrangement within the first tamper resistant barrier (721.34)**

4 Normal English, incorporating the separately defined terms: an Arrangement
   protected by the first Tamper Resistant Barrier, the Arrangement operating as
5 described in the claim.

6 **Prevents the first secure execution space from executing the same executable**
   accessed by a second secure execution space having a second tamper resistant barrier with
7 **a second security level different from the first security level (721.34)**

8 Normal English, incorporating the separately defined terms: stops the first Secure
   Execution Space from executing (e.g. running a program) an Executable accessed
9 by a second Secure Execution space. The first and second Secure Execution
   Spaces have Tamper Resistant Barriers that have different Security Levels.
10

11 **683.2**

12 **First secure container having been received from a second apparatus (683.2)**

13 Normal English, incorporating the separately defined term: the Secure Container
    was acquired from a second apparatus. The second apparatus is different from the
14 first apparatus.

15 **Aspect of access to or use of (683.2, 861.58)**

16 Normal English, incorporating the separately defined terms: Aspect and Access
    to or Use of. Those terms fully define the phrase, so that no other definition is
17 possible.

18 **First secure container rule having been received from a third apparatus different**
    from said second apparatus (683.2)

19 Normal English, incorporating the separately defined terms: this term requires
    that the first Secure Container Rule was acquired from a third apparatus. The
20 third apparatus is different from the second apparatus or the first apparatus.

21 **Hardware or software used for receiving and opening secure containers (683.2)**

22 Normal English, incorporating the separately defined terms: computer hardware
    or programming that acquires Secure Containers and Opens the Secure Containers
23 (see Opening Secure Containers).

24 This phrase has been designated by Microsoft for interpretation under § 112(6).
    InterTrust objects to such designation. Without waiver of such objection, as is
25 required by the Local Rules, InterTrust hereby identifies structures corresponding
    to this term:
26

    Structures corresponding to this element include Processor(s) 4126 and/or
27 software running on Processors 4126 (including Protected Processing
    Environment 650) and Communications Device 666.
28

1   Said secure containers each including the capacity to contain a governed item, a
secure container rule being associated with each of said secure containers (683.2)

2

3   Normal English, incorporating the separately defined terms: the Secure
Containers previously referred to are each able to contain a Governed Item, and
each Secure Container has an associated Secure Container Rule.

4

5   Protected processing environment at least in part protecting information contained
in said protected processing environment from tampering by a user of said first apparatus
(683.2)

6

7   Normal English, incorporating the separately defined terms: a Protected
Processing Environment contains Information. The Protected Processing
Environment protects the contained Information from Tampering by a user. The

8 protection may be partial rather than complete. See Specific Information for the
definition of Information.

9

10   Hardware or software used for applying said first secure container rule and a
second secure container rule in combination to at least in part govern at least one aspect of
access to or use of a governed item contained in a secure container

11 (683.2)

12   Normal English, incorporating the separately defined terms: computer hardware
or programming that uses the first Secure Container Rule and a second Secure

13 Container Rule. These rules are Applied in Combination to Govern a Governed
Item contained in a Secure Container.

14

           This phrase has been designated by Microsoft for interpretation under § 112(6).

15 InterTrust objects to such designation. Without waiver of such objection, as is
required by the Local Rules, InterTrust hereby identifies structures corresponding

16 to this term:

17 Structures corresponding to this element include Processor(s) 4126 and/or software
running on Processors 4126 (including Protected Processing Environment 650).

18

19   Hardware or software used for transmission of secure containers to other
apparatuses or for receipt of secure containers from other apparatuses: (683.2)

20   Normal English, incorporating the separately defined terms: computer hardware
or programming that sends Secure Containers to other apparatuses (e.g., other

21 computers) or acquires Secure Containers from other apparatuses.

22   This phrase has been designated by Microsoft for interpretation under § 112(6).
InterTrust objects to such designation. Without waiver of such objection, as is

23 required by the Local Rules, InterTrust hereby identifies structures corresponding
to this term:

24

           Structures corresponding to this element include Processor(s) 4126 and/or

25 software running on Processors 4126 (including Protected Processing
Environment 650) and Communications Device 666.

26

27

28

303750.01

1   861.58

2   **Creating a first secure container (861.58)**

3   This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements.

4

5   Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following:

6   Normal English, incorporating the separately defined terms: Creating a Secure Container.

7

8   **Including or addressing ... organization information ... desired organization ... and metadata information at least in part specifying at least one step required or desired in creation of said first secure container (861.58)**

9

10   This is not a claim term, but is instead a series of fragments. Interpretation of this phrase is therefore impossible, since the phrase does not appear in the claim.

11   **At least in part determine specific information required to be included in said first secure container contents (861.58)**

12

13   Normal English, incorporating the separately defined terms: at least partially Identify Specific Information that must be included in the first Secure Container.

14   **Rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents (861.58)**

15

16   Normal English, incorporating the separately defined terms: a Rule that Governs at least some of the contents of the Secure Container.

17   **900.155**

18   **First host processing environment comprising (900.155)**

19   A Host Processing Environment including (but not limited to), the listed elements.

20   **Said mass storage storing tamper resistant software (900.155)**

21   Normal English, incorporating the separately defined terms: a mass storage device (e.g., a hard drive) that stores the Tamper Resistant Software.

22

23   **Designed to be loaded into said main memory and executed by said central processing unit (900.155)**

24   Normal English, incorporating the separately defined term: software designed to be loaded into the Memory of a computer and executed by the computer's

25   processor.

26   **Said tamper resistant software comprising: one or more storage locations storing said information (900.155)**

27

28   This is not a claim term, but is instead two sentence fragments. Interpretation of this phrase is therefore impossible, since the phrase does not appear in the claim.

20

303750.01

Derives information from one or more aspects of said host processing environment (900.155)

> Normal English, incorporating the separately defined terms: Derives (including creates) Information based on at least one Aspect of the previously referred to Host Processing Environment. See Specific Information for the definition of Information.

One or more storage locations storing said information (900.155)

> Normal English, incorporating the separately defined terms: Information relating to one or more Aspects of the Host Processing Environment is stored in one or more locations. See Specific Information for the definition of Information.

Information previously stored in said one or more storage locations (900.155)

> See Information Previously Stored. The definitions are the same.

Generates an indication based on the result of said comparison (900.155)

> Normal English: a particular indication is created (e.g., a flag is set or a value is returned) if the comparison has one result, but not if the comparison has a different result.

Programming which takes one or more actions based on the state of said indication (900.155)

> Normal English: software that takes an action if the indication has one state, but does not take that action if the indication does not have that state

At least temporarily halting further processing (900.155)

> Normal English, incorporating the separately defined terms: Halting Processing, the Halt being temporary or permanent. See Securely Processing for the definition of Processing.

912.8

Identifying at least one aspect of an execution space (912.8)

> Normal English, incorporating the separately defined terms: Identifying an Aspect (e.g. Security Level) of an Execution Space

Required for use and/or execution of the load module (912.8)

> Normal English, incorporating the separately defined terms: the Identified Aspect is needed in order for the Load Module to execute or otherwise be used.

Said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security (912.8)

> Normal English, incorporating the separately defined terms: the Execution Space Identifier makes it possible to distinguish higher Security Level Execution Spaces

21

from lower Security level Execution Spaces.

Checking said record for validity prior to performing said executing step (912.8)

Normal English, incorporating the separately defined terms: determining whether the Record has Validity, the determination occurring before the execution step.

912.35

Received in a secure container (912.35)

Normal English, incorporating the separately defined terms: the Record is Contained in a Secure Container when acquired.

Said component assembly allowing access to or use of specified information; (912.35)

Normal English, incorporating the separately defined terms: the Component Assembly allows Access to Specified Information.

Said first component assembly specified by said first record (912.35)

This term is a label referring back to the first component assembly identified earlier in the claim. It has no other meaning.

891.1

Resource processed in a secure operating environment at a first appliance (891.1)

This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements.

Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following:

Normal English, incorporating the separately defined terms: a Resource Processed in a Secure Operating Environment, the Secure Operating Environment being present at an appliance (e.g., a computer).

Securely receiving a first entity's control at said first appliance (891.1)

Normal English, incorporating the separately defined terms: an Entity's Control is Securely Received at the first appliance.

This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term:

Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.

Claim elements specifying the act of "securely receiving" map onto embodiments of "receiving" (see above) in which the received element (e.g., a control) is

22

303750.01

received in a manner providing security. The specification describes a number of security-related mechanisms for use in communications, including encryption, authentication and tamper-resistance. Such mechanisms constitute alternate embodiments.

Securely receiving a second entity's control at said first appliance (891.1)

See Securely receiving a first entity's control at said first appliance. The definitions are the same, except that the second entity and the first entity are different.

Securely processing a data item at said first appliance, using at least one resource (891.1)

Normal English, incorporating the separately defined terms: a Resource is used in Securely Processing a Data Item, the processing occurring at the first appliance.

Securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item (891.1)

Normal English, incorporating the separately defined terms: the first Entity's Control and the second Entity's Control are Securely Applied to Govern Use of the Data Item, the act of Securely Applying involving use of the Resource.

II. Designation of Evidence under 4-2(b).

InterTrust hereby designates the following evidence under Patent Local Rule 4-2 (b), without admission that this constitutes "extrinsic evidence" as defined by the Federal Circuit or other relevant legal authority.

Testimony: Dr. Michael Reiter will testify as to the understanding of the claim terms by someone of ordinary skill in the art.

1. Personal Computer Dictionary (1995) ISBN 0-89218-223-7

   Access
   Copy
   Record

2. Computer Professional's Dictionary, Allen Wyatt (Osborne McGraw-Hill, 1990). ISBN 0-07-881705-6

   Access
   Data Item
   Secure database

3. Microsoft Computer Dictionary, Third Edition (1997) ISBN 1-57231-743-4.

   Addressing
   Copy
   Database
   Data Item

23

1   Environment
     Executable File
2   :
     Load module
3   Memory
     Processing
4   Secure container

5   4. The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992) ISBN 0-395-44895-6

6   Passim

7   5. U.S. Patent No. 5,634,019, Col 7:42-44.
         Secure container

8
     6. Webster's New World Dictionary of Computer Terms, 6th Edition (1997) ISBN 0—02-
9   861890-4

10   Access
         Copy
11   Environment
         Operating environment
12   Secure

13   7. U.S. Patent No. 5,991,399.
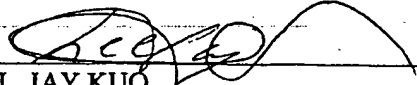
14   Tamper resistant software

15   8. "A Tentative Approach to Constructing Tamper-Resistant Software" by Masahiro
     MAMBO.\Takanori MU RAYAMAT, Fiji OKAMOTO, School of Information Science,
16   Japan Advanced Institute of Science and Technology,1-1 Asahidai Tatsunokuchi Nomi,
     Ishikawa/ 923-1211 Japan, published in English 1998.
17
         Tamper
18   Tamper resistant software

19

20   Dated: December 20, 2002   KEKER & VAN NEST, LLP

21

22

23   By: _____
                                                 L. JAY KUO
                                                 Attorneys for Plaintiff and Counter
24   Defendant
                                                 INTERTRUST TECHNOLOGIES
25   CORPORATION

26

27

28

24

303750.01

PROOF OF SERVICE

I am employed in the City and County of San Francisco, State of California in the office of a member of the bar of this court at whose direction the following service was made. I am over the age of eighteen years and not a party to the within action. My business address is Keker & Van Nest, LLP, 710 Sansome Street, San Francisco, California 94111.

On December 20, 2002, I served the following document(s):

INTERTRUST'S PATENT LOCAL RULE 4-2 PRELIMINARY CLAIM CONSTRUCTIONS AND IDENTIFICATION OF EVIDENCE
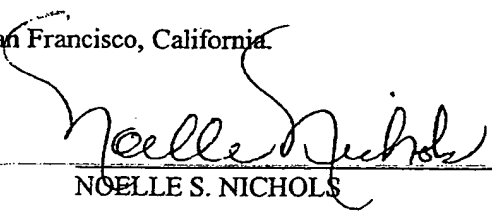
☑ by **PDF TRANSMISSION AND UNITED STATES MAIL,** by transmitting via PDF on this date. A true and correct copy of same was placed in a sealed envelope addressed as shown below. I am readily familiar with the practice of Keker & Van Nest, LLP for collection and processing of correspondence for mailing. According to that practice, items are deposited with the United States Postal Service at San Francisco, California on that same day with postage thereon fully prepaid. I am aware that, on motion of the party served, service is presumed invalid if the postal cancellation date or the postage meter date is more than one day after the date of deposit for mailing stated in this affidavit.

Eric L Wesenberg, Esq.	John D. Vandenberg, Esq.
Mark R. Weinstein, Esq.	James E. Geringer, Esq.
Orrick Herrington & Sutcliffe	Kristin L. Cleveland, Esq.
1000 Marsh Road	Klarquist Sparkman Campbell, et al.
Menlo Park, CA 94025	One World Trade Center, Suite 1600
Telephone: 650/614-7400	121 S.W. Salmon Street
Facsimile: 650/614-7401	Portland OR 97204
	Telephone: 503/226-7391
	Facsimile: 503/228-9446

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Executed on December 20, 2002, at San Francisco, California.

NOELLE S. NICHOLS

303876.01

PROOF OF SERVICE
CASE NO. C01-1640 SBA (MEJ) CONSOLIDATED WITH C 02-0647 SBA

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
HEIDI L. KEEFE (State Bar No. 178960)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650-614-7400
Facsimile: 650-614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: 503-226-7391
Facsimile: 503-228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,
 	
                    Plaintiff,
 	
          v.
 	
MICROSOFT CORPORATION, a Washington corporation,
 	
                    Defendant.
	CASE NO. C01-1640 SBA
	
	MICROSOFT CORPORATION'S PATENT LOCAL RULE 4-2 DISCLOSURE OF PRELIMINARY CLAIM CONSTRUCTION AND EXTRINSIC EVIDENCE (LIMITED TO "MINI-MARKMAN" CLAIMS)

MICROSOFT CORPORATION, a Washington corporation,
 	
                    Counterclaimant,
 	
          v.
 	
INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,
 	
                    Counter Claim-Defendant.	

1   Pursuant to Patent Local Rule 4-2 and this Court's Order, entered November 5, 2002,

2 Defendant Microsoft Corporation ("Microsoft") hereby serves its "Disclosure Of Preliminary

3 Claim Construction And Extrinsic Evidence," limited to the twelve selected "Mini-Markman"

4. patent claims. Microsoft's preliminary claim construction is based upon the proposed terms,

5 phrases and clauses, and claims as a whole, identified by the parties in their submissions in

6 accordance with Patent Local Rule 4-1(a) and conference in accordance with Patent Local Rule 4-

7 1(b).

8   Microsoft provides its preliminary claim construction of each of the 12 "Mini-Markman"

9 claims subject to the limitations and reservations of rights set forth herein. Microsoft does not

10 waive any defenses that the asserted claims fail to satisfy the provisions of 35 U.S.C. § 112

11 including, for example, the written description requirement, the definiteness requirement, or any

12 other requirement for patentability. Microsoft does not concede that the asserted claims are

13 supported by Plaintiff's original application or any application from which they purportedly claim

14 priority. Specifically, by offering a construction of a term, Microsoft does not waive any defense

15 that the claim is in fact indefinite and there can be no proper construction.

16   Microsoft provides its preliminary claim construction in the following format. Exhibit A

17 sets forth Microsoft's preliminary construction of (1) the claim term "virtual distribution

18 environment" ("VDE"), (2) the "VDE invention" disclosed in the February, 1995, InterTrust

19 patent application, and (3) certain other claim terms. Exhibit B sets forth Microsoft's preliminary

20 construction of the disputed claims as a whole, and particular claim phrases in dispute, in the

21 order of appearance in a claim. Where an individual claim term (within a phrase) is also in

22 dispute, it will be bold-faced in Exhibits A and B. Exhibit C sets forth Microsoft's preliminary

23 construction of the individual terms in dispute, in alphabetical order.

24   Microsoft reserves the right to modify its preliminary claim constructions in the event that

25 the parties are unable to agree upon a particular claim construction. Furthermore, because

26 InterTrust has not yet fully complied with the disclosure requirements of Patent Local Rules 3-1

27 and 3-2, Microsoft expressly reserves the right to amend its preliminary claim construction if

28

1   evidence becomes available through those disclosures (or that should have been provided therein)

2   that would support amended constructions. Microsoft further reserves the right to amend its

3   preliminary claim constructions once it has an opportunity to review InterTrust's preliminary

4   claim constructions and once the parties have further met and conferred as required.

5

6   <u>Preliminary Identification of Evidence in Support of Claim Construction</u>

7   Microsoft's preliminary claim construction is supported by the intrinsic record of the

8   seven U.S. patents from which the 12 "Mini-Markman" claims are selected. For the purposes of

9   submission of this preliminary claim construction only, Microsoft treats the "intrinsic" evidence

10 as including: 1) the specifications of each of the seven U.S. patents at issue in the "Mini-

11 Markman" proceeding, including any material purportedly incorporated by reference therein;

12 2) the prosecution history of each of the seven patents at issue, including the applications and

13 prosecution history of the seven patents and any related patent applications, including without

14 limitation, applications purportedly incorporated by reference or to which an application claimed

15 priority; and 3) all references cited in the prosecution of any such applications. In accordance

16 with the local rules, this evidence is not specifically identified, except to the extent that Microsoft

17 asserts particular sections of a patents' specifications provide "structure" for claims properly

18 construed under 35 U.S.C. § 112(6).

19 In certain circumstances, Microsoft's preliminary construction may be supported by

20 extrinsic evidence presently available to Microsoft. Microsoft reserves the right to modify or

21 supplement with evidence that it has not yet been able to fully review, due to InterTrust's

22 production, including without limitation, InterTrust re-production of over 1,000,000 pages on

23 November 4, 2002. Microsoft reserves the right to supplement with additional evidence gathered

24 in the course of the discovery collected between now and the close of "claim construction"

25 discovery or later submitted by InterTrust in full compliance with its disclosure obligations under

26 Patent Local Rules 3-1 and 3-2. Extrinsic evidence is identified or produced in accordance with

27 the local rule and set forth in the following exhibits:

28

MICROSOFT CORPORATION'S PATENT LOCAL
RULE 4-2 DISCLOSURE (LIMITED TO "MINI-
MARKMAN" CLAIMS), CASE No. C 01-1640 SBA

Exhibit D: Contains copies of excerpts from dictionaries and other publications. Due to the volume of the appended pages, Exhibit D will be served via Federal Express.

Exhibit E: Contains a list of selected production documents, identified by initial bates number.

Exhibit F: Contains a list of selected, uncited prior art publications, identified by bates number(s).

Exhbit G: Contains a list of selected, uncited prior art patents, identified by bates number(s).

In addition to the extrinsic evidence cited in Exhibits D-G, Microsoft incorporates by reference herein and reserves the right to rely upon: 1) all documents identified by InterTrust in response to discovery or pursuant to the Patent Local Rules; 2) all InterTrust patents, publications and other things that are prior art to any Mini-Markman claim; and 3) the testimony of InterTrust and the witnesses identified below.

Preliminary Identification of Witnesses[1]

Professor John Mitchell: Dr. Mitchell will testify of the following matters:

1) that certain of the presently disputed terms and phrases used in the twelve claims are amorphous terms lacking a well-defined, precise meaning that can accurately be gleaned from technical or other dictionaries. Rather, these terms are used in the art and/or in the patents in a manner that requires close consideration of the entire patent specification to put them in proper context and determine their precise, correct meaning as used in the patents. These terms include "secure container," "control," "govern," "protect," "protected processing environment," "secure," "securely," "security," "virtual distribution environment";

2) that the concepts stated in the InterTrust patents were known to the art, including the cited prior art, which cited art he will describe;

---

[1] In accordance with the local rules, Microsoft identifies witness testimony that it contends will support its construction. It has not identified herein testimony relevant to the "tutorial" to be held prior to the claim construction hearing.

MICROSOFT CORPORATION'S PATENT LOCAL RULE 4-2 DISCLOSURE (LIMITED TO "MINI-MARKMAN" CLAIMS), CASE NO. C 01-1640 SBA

3) the level of skill, background, and understanding (including extent thereof) of the relevant patent application disclosures by a person of skill in the art; and

4) the meaning and scope certain disputed claim language, including "secure container," "control," "govern," "protect," "protected processing environment," "secure," "securely," "security," and "virtual distribution environment."

Professor David Maier: Dr. Maier will testify on the following matters:

1) what the February 13, 1995, patent application (SN 08/388,107) and the seven InterTrust patents, described as the "invention;" more particularly, what are the required, necessary, non-optional features of the "VDE" "invention" as stated in the patents. This description will include an explanation of the features set forth in Microsoft's "Global Constructions" (Exhibit A).

2) what the February 13, 1995, patent application (SN 08/388,107) and the seven InterTrust patents, required as necessary, non-optional building blocks to implement the "VDE" "invention" as stated in the patents.

Dated: December 20, 2002

By: _____
WILLIAM L. ANTHONY
ERIC L. WESENBERG
HEIDI L. KEEFE
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650-614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: 503-226-7391

MICROSOFT CORPORATION'S PATENT LOCAL RULE 4-2 DISCLOSURE (LIMITED TO "MINI-MARKMAN" CLAIMS), Case No. C 01-1640 SBA

1

2   Attorneys for Defendant
           MICROSOFT CORPORATION
3 Of Counsel:

4 T. Andrew Culbert, Esq.
5 Microsoft Corporation
   One Microsoft Way
6 Building 8
   Redmond, WA 98052-6399
7 Telephone: 425-882-8080

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

MICROSOFT CORPORATION'S PATENT LOCAL
RULE 4-2 DISCLOSURE (LIMITED TO "MINI-
MARKMAN" CLAIMS), CASE No. C 01-1640 SBA

<u>DECLARATION OF SERVICE BY E-MAIL</u>

I am more than eighteen years old and not a party to this action. My place of employment and business address is 121 S.W. Salmon St., Suite 1600, Portland, OR 97204.

On December 20, 2002, at 3:00 p.m., I served on counsel for InterTrust Technologies Corporation:

**MICROSOFT CORPORATION'S PATENT LOCAL RULE 4-2
DISCLOSURE OF PRELIMINARY CLAIM CONSTRUCTION AND
EXTRINSIC EVIDENCE (LIMITED TO "MINI-MARKMAN" CLAIMS)**

by email delivery to:

Michael H. Page, Esq. John W. Keker, Esq. Jon B. Streeter, Esq. Keker & Van Nest, LLP 710 Sansome Street San Francisco, CA 94111 Telephone: 415-391-5400 Facsimile: 415-397-7188 Email: mhp@kvn.com	Douglas Derwin InterTrust Technologies Corporation 4800 Patrick Henry Drive Santa Clara, CA 95054 Telephone: 408-855-0100 Facsimile: 408-855-0144 Email: dderwin@intertrust.com
Steven H. Morrissett, Esq. Finnegan Henderson Farabow Garrett & Dunner Stanford Research Park 700 Hansen Way Palo Alto CA 94304-1016 Telephone: 202-408-4000 Facsimile: 202-408-4400 Email: steven.morrissett@finnegan.com	

I declare under penalty of perjury that the foregoing is true and correct.

Executed on December 20, 2002, at Portland, Oregon.

_____
(SIGNATURE)

_____
Kristin L. Cleveland
(PRINT NAME)

Exhibit A

Below is Microsoft's preliminary construction of the "Virtual Distribution Environment" ("VDE") "invention" of the February 13, 1995, InterTrust application (the "VDE Invention") and certain other terms, which constructions are incorporated by reference into Microsoft's preliminary construction of certain other disputed claims, claim terms, and claim phrases.[1]

Required Feature	Construction
Security and Commerce World	InterTrust's February 13, 1995, patent application described as its "invention" a Virtual Distribution Environment ("VDE invention") for securing, administering, and auditing all security and commerce digital information within its multi-node world (community). VDE guarantees to all VDE "participants" identified in the patent application that it will maintain the **availability**, **secrecy**, **integrity** and **authenticity** of all such information present at any appliance (node) within the VDE world (including protected content (including currency, credit, payments, etc.), information about content usage, content-control **information**, **controls**, **load modules**, etc.). VDE is secure against at least the threats identified in the patent application to this **availability** (no user may delete the information without **authorization**), **secrecy** (neither available nor disclosed to unauthorized persons or processes), **integrity** (neither intentional nor accidental alteration), and **authenticity** (asserted characteristics are genuine). VDE further provides and requires the components and capabilities described below. Anything less than or different than this is not VDE or the described "invention."
VDE Secure Processing Environment	At each node where VDE-protected information is accessed, used, or assigned **control information**, VDE requires a Secure Processing Environment. A Secure Processing Environment is uniquely identifiable, self-contained, non-circumventable, and trusted by all other VDE nodes to protect the **availability**, **secrecy**, **integrity** and **authenticity** of all information identified in the patent application as being protected, and to guarantee that such information will be accessed and used only as expressly authorized by the associated VDE **controls**. A Secure Processing Environment is formed by, and requires, a special-purpose Secure Processing Unit having a hardware **tamper-resistant barrier** encapsulating a processor and internal secure memory. The **barrier** prevents all unauthorized interference, removal, observation, and use of the information and processes within it. A Secure Processing Environment is under control of **controls** and control information provided by one or more parties, rather than being under control of the appliance's users or programs.
VDE Controls	VDE allows access to or use of protected information and processes only through execution of (and satisfaction of the requirements imposed by) independent,

---

[1] The word "invention" is used not to suggest that anything described in InterTrust's patents in fact was novel or non-obvious or inventive, but rather to identify what was described as the alleged invention. Also, features and capabilities are described as they are described in the InterTrust patent application, even though the patent application did not describe an actual working system having any of these capabilities. Also, Microsoft's proposed constructions use many terms from the InterTrust patents that are used inconsistently or otherwise indefinitely in the patents. Those terms are used by Microsoft in their narrowest applicable sense, and without waiving the right to assert the indefiniteness of this claim language. Also, the preliminary constructions assume (without conceding) that the February, 1995, InterTrust patent application was incorporated by reference into the '721, '861, and '683 patents, effectively for claim construction purposes. If the Court concludes otherwise, then the proper constructions will be different in some cases. Bolded terms are preliminarily defined in Exhibits A–C of Microsoft's PLR 4-2 papers.

Required Feature	Construction
	special-purpose, executable VDE control(s). A VDE control can execute only within a Secure Processing Environment. Each VDE control is a component assembly dedicated to a particular activity (e.g., editing, modifying another control, a user-defined action, etc.), particular user(s), and particular protected information. Each separate information access or use is independently controlled by independent VDE control(s). Each VDE control is assembled, within a Secure Processing Environment, from independently deliverable modular components (e.g., load modules or other controls), dynamically in response to an information access or use request. The dynamic assembly of a control is directed by a "blueprint" record (put in place by one or more VDE users) containing control information identifying the exact modular code components to be assembled and executed to govern this particular activity on this particular information by this particular user(s). Each control is independently assembled, loaded and delivered vis-à-vis other controls. Control information and controls are extensible and can be configured and modified by all users, and combined by all users with any other VDE control information or controls (including that provided by other users), subject only to "senior" user controls. Users can assign control information and controls to an arbitrarily fine, user-defined portion of the protected information, such as a single paragraph of a document, as opposed to being limited to file-based controls. VDE controls reliably limit use of the protected information to authorized activities and amounts.
VDE Secure Containers	A VDE secure container is a self-contained, self-protecting data structure which (a) encapsulates information of arbitrary size, type, format, and organization, including other, nested, containers, (b) cryptographically protects that information from all unauthorized access and use, (c) provides encrypted storage management functions for that information, such as hiding the physical storage location(s) of its protected contents, (d) permits the association of itself or its contents with controls and control information governing access to and use thereof, and (e) prevents such use or access (as opposed to merely preventing decryption) until it is opened. A secure container can be opened only as expressly allowed by the associated VDE control(s), only within a Secure Processing Environment, and only through decryption of its encrypted header. A secure container is not directly accessible to any non-VDE calling process. All such calls are intercepted by VDE. The creator of a secure container can assign (or allow others to assign) control information to any arbitrary portion of a secure container's contents, or to an empty secure container (to govern the addition of contents to the secure container, and access to or use of those contents). A container is not a secure container merely because its contents are encrypted and signed. A secure container is itself secure. All VDE-protected information (including protected content, information about content usage, content-control information, controls, and load modules) is encapsulated within a secure container whenever stored outside a Secure Processing Environment or secure database.
Non-Circumventable	VDE is non-circumventable (sequestered). It intercepts all attempts by any and all users, processes, and devices, to access or use (e.g., observe, interfere with, or remove) protected information, and prevents all such attempts other than as allowed by execution of (and satisfaction of all requirements imposed by) associated VDE controls within Secure Processing Environment(s).
Peer to Peer	VDE is peer-to-peer. Each VDE node has the innate ability to perform any role identified in the patent application (e.g., end user, content packager, distributor, clearinghouse, etc.), and can protect information flowing in any direction between any nodes. VDE is not client-server. It does not pre-designate and restrict one or more nodes to act solely as a "server" (a provider of information (e.g., authored content, control information, etc.) to other nodes) or "client" (a requestor of such information). All types of protected-content transactions can proceed without requiring interaction with any server.
Comprehensive Range of	VDE comprehensively governs all security and commerce activities identified in the patent application, including (a) metering, budgeting, monitoring, reporting, and auditing information usage, (b) billing and paying for information usage, and (c) negotiating, signing and enforcing contracts that establish users' rights to

Required Feature	Construction
Functions	access or use information.
User-Configurable	The specific protections governing specific VDE-protected information are specified, modified, and negotiated by VDE's users. For example, VDE enables a consumer to place limits on the nature of content that may be accessed at her node (e.g., no R-rated material) or the amount of money she can spend on viewing certain content, both subject only to other users' senior controls.
General Purpose; Universal	VDE is universal as opposed to being limited to or requiring any particular type of appliance, information, or commerce model. It is a single, unified standard and environment within which an unlimited range of electronic rights protection, data security, electronic currency, and banking applications can run.
Flexible	VDE is more flexible than traditional information security and commerce systems. For example, VDE allows consumers to pay for only the user-defined portion of information that the user actually uses, and to pay only in proportion to any quantifiable VDE event (e.g., for only the number of paragraphs displayed from a book).

Exhibit B

Microsoft PLR 4-2, Exhibit B: Mini Markman Preliminary Claim Construction – Claim Terms[1]

Claim Term	Preliminary Construction
access, accessed, access to, accessing	Establishing the connections, routings, and security requisites needed to physically obtain something. Access to protected information is required, but insufficient, for use of that information. In VDE, access to protected information is achieved only through execution (within a **Secure Processing Environment**) of the VDE control(s) assigned to the particular "access" request, satisfaction of all requirements imposed by such execution, and the controlled opening of the secure container containing the information.
addressing	Referring by specific location or individual name to something without physically storing it.
allowing, allows	Actively permitting an action that otherwise cannot be taken (i.e., is absolutely prohibited) by any user, process, or device. In VDE, an action is allowed only through execution (within a **Secure Processing Environment**) of the VDE control(s) assigned to the particular action request, and satisfaction of all requirements imposed by such execution.
applying . . . in combination	[This shall be construed in connection with a disputed claim phrase.]
arrangement	[This shall be construed in connection with a disputed claim phrase.]
aspect	[This shall be construed in connection with a disputed claim phrase.]
associated with	1. A specific, direct, persistent, and binding relationship with one or more discrete items. Code that processes information but is merely a general-purpose component of an installation is not "associated with" that information. In VDE, an association between a unit of executable code and particular information, or between particular control information and a **secure container**, cannot be broken except as allowed by execution (within a **Secure Processing Environment**) of assigned VDE control(s) and satisfaction of all requirements imposed by such execution. 2. Associations in VDE are created with a component **assembly**, a **secure container**, a **Secure Processing Environment**, "object registration," and other mechanisms of VDE for (allegedly) individually ensuring the "access control" "handcuffs" between specific **controls**, specific objects (and their content at an arbitrary granular level), and specific users.

[1] The word "invention" is used not to suggest that anything described in InterTrust's patents in fact was novel or non-obvious or inventive, but rather to identify what was described as the alleged invention. Also, features and capabilities are described as they are described in the InterTrust patent application, even though the patent application did not describe an actual working system having any of these capabilities. Also, Microsoft's proposed constructions use many terms from the InterTrust patents that are used inconsistently or otherwise indefinitely in the patents. Those terms are used by Microsoft in their narrowest applicable sense, and without waiving the right to assert the indefiniteness of this claim language. Also, the preliminary constructions assume (without conceding) that the February, 1995, InterTrust patent application was incorporated by reference into the '721, '861, and '683 patents, effectively for claim construction purposes. If the Court concludes otherwise, then the proper constructions will be different in some cases. Bolded terms are preliminarily defined in Exhibits A-C of Microsoft's PLR 4-2 papers.

Claim Term	Preliminary Construction
authentication	The act of verifying credentials designed to vouch for the authenticity of the identity, data integrity, and origin integrity of a person, device, program, information, or process.
authorization information, authorized, not authorized	authorized: An action is permitted that otherwise cannot be taken (i.e., is absolutely prohibited) by any user, process, or device. In VDE, an action is authorized only through execution of the applicable VDE control(s) within a VDE Secure Processing Environment and satisfaction of all requirements imposed by such execution. authorization information: "Control information" identifying the exact modular code components to be assembled into a VDE control and executed within a Secure Processing Environment to permit a particular activity that otherwise cannot be taken (i.e., is absolutely prohibited). ("Control information" is information which identifies the exact modular code components and data which must be assembled and executed to control a particular activity on particular information, of arbitrary, user-defined granularity, by particular user(s)). "not authorized": The action is prohibited and cannot be taken by any user, process, or device.
budget control; budget	budget: A unique type of "method" that specifies limitations on future usage (e.g., copying) of digital information and how such usage will be paid for, if at all. (A "method" is a collection of basic instructions, and information related to basic instructions, that provides context, data, requirements, and/or relationships for use in performing, and/or preparing to perform, basic instructions in relation to the operation of one or more electronic appliances.) budget control: A VDE control assembled using a budget, and enforcing that budget. No process, user, or device is able to make the use identified by the budget once the budget's specified limitation on that use has been met.
can be	Something is permitted that otherwise cannot happen (i.e., is absolutely prohibited).
capacity	Available storage space that is still capable of allocation. For example, a 650 MB blank CD, after sealing, has zero capacity because no new material may be stored within it.
clearinghouse	A computer system that provides intermediate storing and forwarding services for both content and audit information, and which two or more parties trust to provide its services independently because it is operated under constraint of VDE security. "Audit information" means all information created, stored, or reported in connection with an "auditing" process. "Auditing" means tracking, metering and reporting the usage of particular information or a particular appliance.
compares, comparison	A processor operation that evaluates two quantities and sets one of three flag conditions as a result of the comparison – greater than, less than, equal to.
component assembly (2)	A cohesive executable component created by a channel which binds or links together two or more independently deliverable load modules, and associated data. A component assembly is assembled, and executes only within a VDE Secure Processing Environment. A component assembly is assembled dynamically in response to, and to service, a particular content-related activity (e.g., use request). Each VDE component assembly is assigned and dedicated to a particular activity, particular user(s), and particular protected information. Each component assembly is independently

Claim Term	Preliminary Construction
	assembled, loadable and deliverable vis-à-vis other component assemblies. The dynamic assembly of a component assembly is directed by a "blueprint" record containing control information for this particular activity on this particular information by this particular user(s). Component assemblies are extensible and can be configured and reconfigured (modified) by all users, and combined by all users with other component assemblies, subject only to other users' "senior" controls.
contain, contained, containing	Physically storing within, as opposed to addressing.
control (n.), controls (n.) (2 – 193:1,11,15,19; 891:1)	VDE allows access to or use of protected information only through execution of (and satisfaction of the requirements imposed by) independent, special-purpose, executable VDE control(s). A VDE control can execute only within a Secure Processing Environment. Each VDE control is a component assembly dedicated to a particular activity (e.g., editing, modifying another control, a user-defined action, etc.), particular user(s), and particular protected information. Each separate information access or use is independently controlled by independent VDE control(s). Each VDE control is assembled within a Secure Processing Environment from independently deliverable modular components (e.g., load modules or other controls), dynamically in response to an information access or use request. The dynamic assembly of a control is directed by a "blueprint" record (put in place by one or more VDE users) containing control information identifying the exact modular code components to be assembled and executed to govern this particular activity on this particular information by this particular user(s). Each control is independently assembled, loaded and delivered vis-à-vis other controls. Control information and controls are extensible and can be configured and modified by all users, and combined by all users with any other VDE control information or controls (including that provided by other users), subject only to "senior" user controls. Users can assign control information (including alternative control information) and controls to an arbitrarily fine, user-defined portion of the protected information, such as a single paragraph of a document, as opposed to being limited to file-based controls. VDE controls reliably limit use of the protected information to authorized activities and amounts.
controlling, control (v.)	1. Reliably defining and enforcing the conditions and requirements under which an action that otherwise absolutely cannot be taken, will be allowed, and the manner in which it may occur. Absent verified satisfaction of those conditions and requirements, the action cannot be taken by any user, process or device. In VDE, an action is controlled through execution of the applicable VDE control(s) within a VDE Secure Processing Environment.

2. More specifically, in VDE, controlling is effected by use of VDE controls, VDE secure containers, and VDE foundation (including VDE Secure Processing Environment, "object registration," and other mechanisms for allegedly individually ensuring that specific controls are enforced vis-à-vis specific objects (and their content at an arbitrary granular level) and specific "users.") |
| copied file | A digital file which has been copied at least once, not the copy itself. A "copy" is what is formed by a copying operation, and it may or may not be encrypted, ephemeral, usable, or accessible. |
| copy, copied, copying (v.) | To duplicate a digital file or other complete physical block of data from one location on a storage medium to another location on the same or different storage medium, leaving the original block of data unchanged, such that two distinct and independent objects exist. Although the layout of the data values in physical storage may differ from the original, the resulting "copy" is logically indistinguishable from the original. The resulting "copy" may or |

Claim Term	Preliminary Construction
	may not be encrypted, ephemeral, usable, or accessible.
copy control	A VDE control which controls some access to or use of a copy.
creating, creation	[This shall be construed in connection with a disputed claim phrase.]
data item	An individual unit of information representing a single value, such as that stored in a field of a larger record in a database. It is the smallest useful unit of named information in the system.
derive, derives	To retrieve from a specified source.
descriptive data structure	A machine-readable data structure (e.g., text file, template, secure container, etc.) containing or addressing descriptive information (e.g., metadata, shorthand abstract representation, integrity constraints, rules, instructions, etc.) about (1) the layout, generic format (e.g., location of a particular type of information), attributes, or hierarchical structure (e.g., file hierarchy) of the contents section of one or a family of other data structure(s) (e.g., secure container, other rights management related structure, etc.), (2) the operations or processes used to create or use such other data structure(s) (e.g., rules for handling the data structure), and/or (3) the consequences of such operations (e.g., billing the user a certain fee for printing). The descriptive data structure is capable of being used to create or handle (e.g., read, locate information within, request information from, and/or manipulate) the other data structure(s). The descriptive data structure is not associated with the other data structure(s) and does not contain or specify its particular contents (e.g., "Yankees Win the Pennant!").
designating	[This shall be construed in connection with a disputed claim phrase.]
device class	The generic name for a group of device types. For example, all display stations belong to the same device class. A device class is different from a device type. A device type is composed of all devices that share a common model number or family (e.g. IBM 4331 printers).
digital file	A static unit of storage allocated by a "file system" and containing digital information. A digital file enables any application using the "file system" to randomly access its contents and to distinguish it by name from every other such unit. A copy of a digital file is a separate digital file. (A "file system" is the portion of the operating system that translates requests made by application programs for operations on "files" into low-level tasks that can control storage devices such as disk drives.)
digital signature, digitally signing	digital signature: An unforgable string of characters (e.g., bits) generated by a cryptographic transformation to a block of data using some secret, which string can be generated only by an agent that knows the secret, and hence provides evidence that the agent must have generated it. digitally signing: Creating a digital signature using a secret key. (In symmetric key cryptography, a "secret key" is a key that is known only to the sender and recipient. In asymmetric key cryptography, a "secret key" is the private key of a public/private key pair, in which the two keys are related uniquely by a predetermined mathematical relationship such that it is computationally infeasible to determine one from the other.)
entity, entity's control	entity: Any person or organization.

Claim Term	Preliminary Construction
	entity's control: Control created, modified, or selected by any person or organization to control a particular use of or access to particular protected information by a particular user(s).
environment	[This will be construed in connection with other disputed claim terms.]
executable programming, executable (2)	executable: A cohesive series of machine code instructions in a format that can be loaded into memory and run (executed) by a connected processor. executable programming: A cohesive series of machine code instructions, comprising a computer program, in a format that can be loaded into memory and run (executed) by a connected processor. (A "computer program" is a complete series of definitions and instructions that when executed on a computer will perform a required or requested task.)
execution space, execution space identifier	execution space: A processor-addressable physical memory into which data and executable code can be loaded, which is assigned to a single executing process while that process is actively executing. Memory holding "swapped out" processes or executables is not part of an "execution space." execution space identifier: A value that uniquely identifies a particular execution space.
generating	[This shall be construed in connection with a disputed claim phrase.]
govern, governed, governed item, governing	govern, governing, governed: See control (v). governed item: Information, of arbitrarily fine granularity, whose access and use by any user, process, or device which is controlled.
halting	Stopping execution of a running (executing) process unconditionally (i.e., without providing any specific condition for resumption). For example, executing an instruction known as a "breakpoint halt instruction."
host processing environment	A processing environment within a VDE node which is not a Secure Processing Environment. A "host processing environment" may either be "secure" or "not secure." A "secure" host processing environment is a self-contained protected processing environment, formed by loaded, executable programming executing on a general purpose CPU (not a Secure Processing Unit) running in protected (privileged) mode. A "non-secure" host processing environment is formed by loaded, executable programming executing on a general purpose CPU (not a Secure Processing Unit) running in user mode.
identifier, identify, identifying	identifier: Any text string used as a label naming an individual instance of what it identifies. identify: To establish as being a particular instance of a person or thing.
including	(With respect to a digital file, control, authorization information, Secure Processing Environment, descriptive data structure, element, load module, header, or secure container): Physically storing within, as opposed to addressing.
information previously stored	Information that once was stored but is no longer stored.

Claim Term	Preliminary Construction
integrity programming	Executable programming that when executed checks and reports on the integrity of a device or process. "Integrity" means the property that information has not been altered either intentionally or accidentally.
key	A bit sequence used and needed by a cryptographic algorithm to encrypt a block of plain text or to decrypt a block of cipher text. A key is different from a key seed or other information from which the actual encryption and/or decryption key is constructed, derived, or otherwise identified. In symmetric key cryptography, the same key is used for both encryption and decryption. In asymmetric or "public key" cryptography, two related keys are used; a block of text encrypted by one of the two keys (e.g., the "public key") can be decrypted only by the corresponding key (e.g., the "private key").
load module ②	An executable, modular unit of machine code suitable for loading into memory for execution by a processor. A load module is encrypted (when not within a Secure Processing Unit) and has an identifier that a calling process must provide to be able to use the load module. A load module is combinable with other load modules, and associated data, to form executable component assemblies. A load module can execute only in a VDE protected processing environment.
machine check programming	Executable programming that when executed generates a unique "machine signature" which distinguishes the physical machine from all other machines. This machine check programming code sometimes is invoked by integrity programming.
metadata information ② (metadata))	Data that describes other data managed within an application or environment, such as its meaning, representation in storage, what it is used for and by whom, context, quality and condition, or other characteristics. Metadata may describe data elements or attributes (name, size, data type, etc) and data about records or data structures (length, fields, columns, etc) and data about data (where it is located, how it is associated, ownership, etc.).
opening secure containers	Establishing the requisites needed to attempt to access the contents of a secure container. Opening is a necessary but insufficient step before the contents of a secure container may be copied, decrypted, read, manipulated, or otherwise used, or accessed. No process, user, or device may access or use the contents of a secure container without first opening that secure container. A secure container may be opened only through execution of the assigned VDE control(s) within a VDE Secure Processing Environment and satisfaction of all requirements imposed by such execution.
operating environment	See processing environment.
organization, organization information, organize	organization, organization information: The manner in which data is represented and laid out in physical storage. For example, for data organized as records: the field hierarchy, order, type and size. organize: Representing and laying out data in a particular manner in physical storage.
portion	[This shall be construed in connection with a disputed claim phrase.]
prevents	Imposes an active restraint on an action such that it absolutely cannot occur by any means or under any circumstances.
processing environment (2 – 912:35, 900:155, 721:34)	A standardized, well-defined, self-contained, computing base, formed by hardware and executing code, that provides an "interface" and set of resources which can support different applications, on different types of hardware platforms. In the context of claim 35 of the '912 patent: a Secure Processing

Claim Term	Preliminary Construction
	Environment.
protected processing environment (2 – 721:34)	1. A uniquely identifiable, self-contained computing base trusted by all VDE nodes to protect the **availability, secrecy, integrity and authenticity of all** information identified in the patent application as being protected, and to guarantee that such information will be **accessed and used only as expressly** authorized by VDE controls. At most VDE nodes, the protected processing environment is a Secure Processing Environment which is formed by, and requires, a hardware **tamper-resistant barrier encapsulating a special-purpose Secure Processing Unit having a processor and internal secure** memory. ("Encapsulated" means hidden within an object so that it is not directly accessible but rather is accessible only through the object's restrictive interface.) The **barrier prevents all unauthorized** (intentional or accidental) interference, removal, observation, and **use of the information and** processes within it, by all parties (including all users of the device in which the Protected Processing Environment resides), except as expressly **authorized by VDE controls.** A Protected Processing Environment is under control of controls and control information provided by one or more parties, rather than being under control of the appliance's users or programs. Where a VDE node is an established financial clearinghouse, or other such facility employing physical facility and user-identity authentication security procedures trusted by all VDE nodes, and the VDE node does not access or use VDE-protected information, or assign VDE **control information,** then the Protected Processing Environment at that VDE node may instead be formed by a **géneral-purpose** CPU that executes all VDE "**security**" processes in protected (privileged) mode.

2. A Protected Processing Environment requires more than just verifying the **integrity of digitally signed executable programming prior to execution** of the programming; or concealment of the program, associated data, and execution of the program code; or use of a password as its protection mechanism. |
protecting	Maintaining the security of.
record (n.)(2)	A data structure that is a collection of fields (elements), each with its own name and type. Unlike an array, whose elements are accessed using an index, the elements of a record are accessed by name. A record can be accessed as a collective unit of elements, or the elements can be accessed individually.
required	A condition without which an action cannot occur. A required condition acts prospectively – it does not apply to a description created at or after the creation of the object to which it applies.
resource processed	A record containing **control information, which record** is stored and acted upon within a processing environment.
rule (2) --	A lexical statement that states a condition under which access to or use of VDE-protected data will be allowed by a VDE control. A rule may specify how, when, where, and by whom a particular activity on particular information is to be allowed.
secure (2)	A state in which all users of a system are guaranteed that all **information, processes, and devices within the system, shall have their availability, secrecy,** **integrity and authenticity** maintained against all of the identified threats thereto. "**Availability**" means the property that information is accessible and usable upon demand by authorized persons, at least to the extent that no user may delete the information without authorization. "**Secrecy,**" also referred to as confidentiality, means the property that information (including computer processes) is not made available or disclosed to unauthorized persons or processes. "**Integrity**" means the property that information has not been altered either intentionally or accidentally. "**Authenticity**" means the

Claim Term	Preliminary Construction
	property that the characteristics asserted about a person, device, program, information, or process are genuine and timely, particularly as to identity, data integrity, and origin integrity.
secure container	A VDE secure container is a self-contained, self-protecting data structure which (a) encapsulates information of arbitrary size, type, format, and organization, including other, nested, containers, (b) cryptographically protects that information from all unauthorized access and use, (c) provides encrypted storage management functions for that information, such as hiding the physical storage location(s) of its protected contents, (d) permits the association of itself or its contents with controls and control information governing access to and use thereof, and (e) prevents such use or access (as opposed to merely preventing decryption) until it is "opened." A secure container can be opened only as expressly allowed by the associated VDE control(s), only within a Secure Processing Environment, and only through decryption of its encrypted header. A secure container is not directly accessible to any non-VDE or user calling process. All such calls are intercepted by VDE. The creator of a secure container can assign (or allow others to assign) control information to any arbitrary portion of a secure container's contents, or to an empty secure container (to govern the later addition of contents to the container, and access to or use of those contents). A container is not a secure container merely because its contents are encrypted and signed. A secure container is itself secure. All VDE-protected information (including protected content, information about content usage, and content-control information, controls, and load module) is encapsulated within a secure container whenever stored outside a Secure Processing Environment or secure database.
secure container governed item	A governed item protected by a secure container. A secure container governed item may not be accessed or used in any way, by any user, process, or device, except as allowed by its associated VDE control(s) executing in a VDE Secure Processing Environment and satisfaction of all requirements imposed by such execution.
secure container rule	A rule protected by a secure container. A secure container rule may not be accessed or used in any way, by any user, process, or device, except as allowed by its associated VDE control(s) executing in a VDE Secure Processing Environment and satisfaction of all requirements imposed by such execution.
secure database	A data store isolated from all users such that it is protected from external observation; and accidental or intentional alteration or destruction. In VDE, a secure database stores tracking, billing, payment, and auditing data until the data is delivered securely to an authorized clearinghouse.
secure execution space	An allocated portion of the secure memory within a special-purpose Secure Processing Unit which is isolated from the rest of the world, and protected from observation by (and encapsulated within) a tamper resistant barrier and protected from alteration by the processor. The processor cryptographically verifies the integrity of all code loaded from secure memory prior to execution, executes only the code that the processor has authenticated for its use, and is otherwise secure.
secure memory, memory	memory: A medium in which data (including executable instructions) may be stored and from which it may be retrieved. "Memory" does not include a "virtual memory." secure memory: A processor-addressable memory within a special-purpose Secure Processing Unit which is isolated from the rest of the world by (and encapsulated within) a tamper resistant barrier. "Processor-addressable" means that a connected processor can use the secure memory's

Claim Term	Preliminary Construction
	physical addresses as the operand in a processor instruction such as LOAD or STORE or equivalent instruction. A "memory" is not a "secure memory" merely because it stores encrypted, signed, and/or sealed data; is accessible from a Protected Processing Environment; or is within an appliance that is located at a trusted facility with non-VDE physical security and user-identity authentication procedures.
secure operating environment, said operating environment	Same as Secure Processing Environment.
securely applying (2 – securely)	securely: Performed in a Secure Processing Environment in a manner that guarantees that each affected information or process remains secure. securely applying: securely (1) executing the applied executables (e.g., controls) within a VDE secure execution space, (2) validating and verifying the authenticity and integrity of each executable, and (3) ensuring that the executables are applied only in ways that are intended by the VDE participants who created the executables.
securely assembling	securely (1) linking or binding plural distinct elements together in a particular manner (specified by authenticated assembly instructions) into a single cohesive executable unit so the elements can directly reference each other element within the resulting assembly, within a VDE Secure Processing Environment, (2) validating and verifying the authenticity and integrity of each element (e.g., that it has not been modified from or substituted for the correct element) immediately prior to binding it into the assembly, and (3) ensuring that the elements are linked together only in ways that are intended by the VDE participants who created the elements and/or specified the assembly thereof.
securely processing	Executing code in a secure execution space to act upon some information, in a manner that ensures that the information and the processing remain secure.
securely receiving	Receiving digital information in a secure container, as part of a communication encrypted on the communications level, at a Secure Processing Environment authenticated in accordance with VDE controls associated with the secure container.
security (2)	See secure.
security level, level of security	An ordered measure of the degree of security. The "security level" is persistent unless expressly noted to exist only some of the time. Also, the combination of a hierarchical classification and a set of nonhierarchical categories that represents the sensitivity of an object or the clearance of a subject. For example, Unclassified, Confidential, Secret, and Top Secret are hierarchical classifications, whereas NATO and NOFORN are non-
specific information, specified information	[This will be construed in connection with disputed claim phrases]
tamper resistance (2 – tamper)	tamper resistance: The ability of a tamper resistant barrier to prevent access, observation, and interference with information or processing encapsulated by the barrier.

Page 9 of 10

Claim Term	Preliminary Construction
	tamper: See tampering.
tamper resistant barrier	An active device that encapsulates and separates a Protected Processing Environment from the rest of the world. It prevents information and processes within the Protected Processing Environment from being observed, interfered with, and leaving except under appropriate conditions ensuring security. It also controls external access to the encapsulated secure resources, processes and information. A tamper resistant barrier is capable of destroying protected information in response to tampering attempts.
tamper resistant software	Software that is encapsulated and executed wholly within a tamper resistant barrier.
tampering (2)	Attempting to circumvent a tamper resistant barrier or other mechanism designed to protect against the observation, access, or alteration of data, code, or process execution, or making any unauthorized access, observation, or interference.
use (n.)	Any action with respect to information (e.g., copying, printing, decrypting, executing) other than access. In VDE, information use is allowed only through execution of the applicable VDE control(s) and satisfaction of all requirements imposed by such execution.
user controls (1)	Controls created, modified, or selected by a user to control a particular use or access by the user to particular protected information.
validity	The state in which authenticated data conforms to predetermined completeness and consistency parameters.
virtual distribution environment	See Global Construction of VDE.

Exhibit C

Microsoft PLR 4-2, Exhibit C: Mini Markman Preliminary Claim Construction -- Claim Phrases[1]

Claim Phrase	Microsoft's Preliminary Construction
'193:1	**Claim as a Whole:** The recited method is performed within a VDE.
receiving a digital file including music	1. This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites a step or result ("receiving") without reciting an action that achieves that result. The specification does not clearly link any particular action to this recited step. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b).
	2. The qualifier "including music" recites a non-functional descriptive material and is not a patentable limitation.
	3. The recited function requires: obtaining a VDE secure container encapsulating a digital file, authenticating the intended recipient in accordance with VDE controls associated with the secure container, and accepting the secure container.
a budget specifying the number of copies which can be made of said digital file	1. A budget identifying the total number of copies (whether or not decrypted, long-lived, or accessible) that (since creation of the budget) can be made of the digital file by any and all users, devices, and processes. No process, user, or device is able to make another copy of the digital file once this number of copies has been made.
controlling the copies made of said digital file	1. Controlling uses of and accesses to all copies of the digital file, by all users, processes, and devices, by executing each of the recited "at least one" copy control(s) within VDE Secure Processing Environment(s). Each control governs (controls) only one action, which action may or may not differ among the different "at least one" controls. All uses and accesses are prohibited and incapable of occurring except to the extent allowed by the "at least one" copy control(s).
determining whether said digital file may be copied and stored on a second device based on at least said copy control	1. Determining whether this particular first device is allowed to perform both of the following actions on this particular digital file: (1) copy it and (2) store it (as opposed to a copy of it) on a second device, by executing one or more VDE control(s) (including "said" copy control associated with this digital file) within VDE Secure Processing Environment(s). To the extent that either of these two actions is not determined by this step to be permissible, that action is absolutely prohibited and incapable of occurring, and no user, process or device can perform it on this digital file.

[1] The word "invention" is used not to suggest that anything described in InterTrust's patents in fact was novel or non-obvious or inventive, but rather to identify what was described as the alleged invention. Also, features and capabilities are described as they are described in the InterTrust patent application, even though the patent application did not describe an actual working system having any of these capabilities. Also, Microsoft's proposed constructions use many terms from the InterTrust patents that are used inconsistently or otherwise indefinitely in the patents. Those terms are used by Microsoft in their narrowest applicable sense, and without waiving the right to assert the indefiniteness of this claim language. Also, the preliminary constructions assume (without conceding) that the February, 1995, InterTrust patent application was incorporated by reference into the '721, '861, and '683 patents, effectively for claim construction purposes. If the Court concludes otherwise, then the proper constructions will be different in some cases. Bolded terms are preliminarily defined in Exhibits A-C of Microsoft's PLR 4-2 papers.

Claim Phrase	Microsoft's Preliminary Construction
	2. This claim limitation's recitation of "said" copy control is inconsistent with the claim limitation "at least one" copy control.
if said copy control allows at least a portion of said digital file to be copied and stored on a second device	1. This "if" condition creates two branches for the recited process, each of which must be performed. Each time the "if" condition is met, all four of the later-recited actions (copying, transferring, storing, playing) must occur. Each time it is not met, each of these four actions must be prohibited and incapable of occurring.
	2. This "if" condition is met if and only if "said" copy control allows any portion of the digital file to be copied and also allows that same portion of the file (as opposed to the copy) to be stored on any second device. This "if" condition is based entirely on "said copy control" and thus is met, as above, even if other VDE control(s) prohibit those actions.
	3. This claim limitation's recitation of "copy control allows at least a portion" is inconsistent with the claim limitation "whether said digital file may be copied ... based on at least said copy control."
copying at least a portion of said digital file	1. Copying at least some portion of the digital file (as opposed to a copy thereof), by executing VDE control(s) within VDE Secure Processing Environment(s). This copied "portion" may or may not be (or even include) the portion referred to in the claim limitation "if said copy control allows at least a portion."
transferring at least a portion of said digital file to a second device	1. Transferring to some second device (which may or may not be the "second device" referred to in the claim limitation "if said copy control allows at least a portion of said digital file to be copied and stored on a second device") at least some portion of the digital file (as opposed to a copy thereof), by executing VDE control(s) within VDE Secure Processing Environment(s). This transferred portion may or may not be (or even include) the portion referred to in the claim limitation "if said copy control allows at least a portion," or the portion referred to in the claim limitation "copying at least a portion."
storing said digital file	1. Storing the entire digital file received in the "receiving" step (as opposed to a copy of the file or an incomplete portion of the file).
	2. This claim limitation's recitation of "storing said digital file" is inconsistent with the claim limitation "transferring at least a portion of said digital file."
'193:11	Claim as a Whole: The recited method is performed within a VDE.
receiving a digital file	1. This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites a step or result ("receiving") without reciting an action that achieves that result. The specification does not clearly link any particular action to this recited step. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b).
	2. The recited function requires: obtaining a VDE secure container encapsulating a digital file, authenticating the intended recipient in accordance with VDE controls associated with the secure container, and accepting the secure container.
determining whether said digital file may be copied	1. Determining whether said first control, by itself, allows this particular first device to perform both of the following actions on this particular digital file: (1) copy it and (2) store it (as opposed to a copy of it) on a second device, by executing the first VDE control within VDE Secure Processing

Claim Phrase	Microsoft's Preliminary Construction
and stored on a second device based on said first control	Environment(s). To the extent that either the copy or store action is not determined by this step to be permissible, that action is absolutely prohibited and incapable of occurring, and no user, process or device can perform it on this digital file.
identifying said second device	1. Identifying a second device sufficiently to distinguish it from all other devices, by executing VDE control(s) within VDE Secure Processing Environment(s).
whether said first control allows transfer of said copied file to said second device	1. Whether the first control, by itself, allows the entire digital file (which has been copied at least once) (as opposed to the copy) to be moved to the identified second device. If not, that transfer is absolutely prohibited and incapable of occurring and no user, process or device can perform that action on this file.
said determination based at least in part on the features present at the device	1. Basing the determination at least in part upon all actual, current features of the device (as opposed to previously determined, reported, or measured features) which might affect the device's ability to prevent unauthorized access to and/or use of the digital file. This determination is done without trusting either the device or any user of the device. A device identifier such as a serial number is not a "feature present at the device."
if said first control allows at least a portion of said digital file to be copied and stored on a second device	1. This "if" condition creates two branches for the recited process, each of which must be performed. Each time the "if" condition is met, all four of the later-recited actions (copying, transferring, storing, rendering) must occur. Each time it is not met, each of these four actions must be disabled and prohibited and incapable of occurring.
	2. This "if" condition is met if and only if the first control allows any portion of the digital file to be copied and also allows that same portion of the file (as opposed to the copy) to be on any second device. This "if" condition is based entirely on the first control and thus is met, as above, even if other VDE controls prohibit those actions.
	3. This claim limitation's recitation of "said first control allows at least a portion" is inconsistent with the claim limitation "whether said digital file may be copied ... based on said first control."
copying at least a portion of said digital file	1. Copying at least some portion of the digital file (as opposed to a copy thereof), by executing VDE control(s) within VDE Secure Processing Environment(s). The copied portion may or may not be (or even include) the portion referred to in the claim limitation "if said first control allows at least a portion."
transferring at least a portion of said digital file to a second device	1. Transferring to some second device (which may or may not be the "second device" referred to in the claim limitation "if said first control allows at least a portion of said digital file to be copied and stored on a second device") at least some portion of the digital file (as opposed to a copy thereof), by executing VDE control(s) within VDE Secure Processing Environment(s). The transferred portion may or may not be (or even include) the portion referred to in the claim limitation "if said first control allows at least a portion," or the portion referred to in the claim limitation "copying at least a portion."
storing said digital file	1. Storing the entire digital file received in the "receiving" step (as opposed to a copy of the file or an incomplete portion of the file).

Claim Phrase	Microsoft's Preliminary Construction
	2. This claim limitation's recitation of "storing said digital file" is inconsistent with the claim limitation "transferring at least a portion of said digital file."
'193:15	Claim as a Whole: The recited method is performed within a VDE.
receiving a digital file	1. See 193:11. This step must proceed in both "authentication branches" of the process (i.e., regardless of the outcome of the "authentication" step).
an authentication step comprising:	1. Authenticating the first device and/or user of the first device without relying on trusting either, by executing VDE control(s) within VDE Secure Processing Environment(s).
accessing at least one identifier associated with a first device or with a user of said first device	1. Securely accessing at least one identifier associated with a single ("first") device or (as opposed to "and") with a single, current user of that device, by executing VDE control(s) within VDE Secure Processing Environment(s). One of the "at least one identifier" may be associated with a first device while another of the "at least one identifier" may be associated with a user of said first device.
determining whether said identifier is associated with a device and/or user authorized to store said digital file	1. For each accessed "at least one identifier," determining whether the device with which it is associated is one on which the file may be stored (by any user) and/or whether the user with which it is associated is one who may store the file (on any device), by executing VDE control(s) within VDE Secure Processing Environment(s). Each identifier may be associated with a device "and" a user, or with a device only, or with a user only. 2. This claim limitation's recitation of "said identifier" is inconsistent with the claim limitation "at least one identifier."
storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized	1. This conditional step creates at least two "authentication" branches for the recited process, each of which must be performed. Each time the condition is met, the recited "storing" must occur. Each time it is not met, the recited "storing" must not occur. 2. If "storing" proceeds, then: storing in a secure memory of the first device, the entire file received in the "receiving" step, as opposed to a copy of the file or an incomplete portion of the file, by executing VDE control(s) within VDE Secure Processing Environment(s). If "storing" does not proceed: then the file is not stored in the secure memory of the first device, and is absolutely prevented from being stored anywhere on the first device. 3. This limitation is internally inconsistent on the circumstances under which the storing proceeds or does not proceed. For example, the first ("only if") phrase requires that the storing step proceeds if the device is authorized (and the user is not) while the second ("but not") phrase requires that the storing step not proceed if the device is authorized (and the user is not).
storing information associated with said digital file in a secure database stored on said first device, said information including	1. Storing information in a secure database, the entirety of information (including the "at least one control") being associated with the digital file (as opposed to the file's contents independent of the file), by executing VDE control(s) within VDE Secure Processing Environment(s). 2. This step must proceed in both "authentication branches" of the process (i.e., regardless of the outcome of the "authentication" step).

Claim Phrase	Microsoft's Preliminary Construction
at least one control	
determining whether said digital file may be copied and stored on a second device based on said at least one control	1. Determining whether the "at least one control," by itself or themselves, allow(s) this particular first device to perform both of the following actions on this particular digital file: (1) copy it and (2) store it (as opposed to a copy of it) on a second device, by executing "said at least one control," by executing the "at least one" VDE control within VDE Secure Processing Environment(s). To the extent that either the copy or store action is not determined by this step to be permissible, that action is absolutely prohibited and incapable of occurring, and no user, process or device can perform it on this digital file. 2. This step must proceed in both "authentication branches" of the process (i.e., regardless of the outcome of the "authentication" step).
if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,	1. This "if" condition creates two branches for each of the two "authentication branches" of the recited process (and thus four branches in all), each of which must be performed. Each time it is met, all four of the later-recited actions (copying, transferring, storing, rendering) must occur. Each time it is not met, each of these four actions must be prohibited and incapable of occurring. 2. This "if" condition is met if and only if the at least one control allows any portion of the digital file to be copied and also allows that same portion of the file (as opposed to the copy) to be stored on any second device. This "if" condition is based entirely on the at least one control and thus is met, as above, even if other VDE controls prohibit those actions. 3. This step must proceed in both "authentication branches" of the process (i.e., regardless of the outcome of the "authentication" step). 4. This claim limitation's recitation of "at least one control allows at least a portion of said digital file" is inconsistent with the claim limitation "whether said digital file may be copied ... based on said at least one control."
copying at least a portion of said digital file	1. Copying at least some portion of the digital file (as opposed to a copy thereof), which portion may or may not be (or even include) the portion referred to in the claim limitation "if said at least one control allows at least a portion," by executing VDE control(s) within VDE Secure Processing Environment(s). 2. This step must proceed in both "authentication branches" of the process (i.e., regardless of the outcome of the "authentication" step).
transferring at least a portion of said digital file to a second device	1. Transferring to some second device (which may or may not be the "second device" referred to in the claim limitation "if said at least one control allows at least a portion of said digital file to be copied and stored on a second device") at least some portion of the digital file (not a copy thereof), by executing VDE control(s) within VDE Secure Processing Environment(s). The transferred portion may or may not be (or even include) the portion referred to in the claim limitation "if said at least one control allows at least a portion," or the portion referred to the claim limitation "copying at least a portion." 2. This step must proceed in both "authentication branches" of the process (i.e., regardless of the outcome of the "authentication" step).
storing said digital file	1. Storing the entire digital file received in the "receiving" step (as opposed to a copy of the file or an incomplete portion of the file).

Claim Phrase	Microsoft's Preliminary Construction
	2. This step must proceed in both "authentication branches" of the process (i.e., regardless of the outcome of the "authentication" step). 3. This claim limitation's recitation of "storing said digital file" is inconsistent with the claim limitation "transferring at least a portion of said digital file."
'193:19	**Claim as a Whole:** The recited method is performed within a VDE.
receiving a digital file at a first device	1. This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites a step or result ("receiving") without reciting an action that achieves that result. The specification does not clearly link any particular action to this recited step. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b). 2. The recited function requires: obtaining a VDE secure container encapsulating a digital file, authenticating the first device in accordance with VDE controls associated with the secure container, and accepting the secure container.
establishing communication between said first device and a clearinghouse located at a location remote from said first device	1. This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites a step or result ("establishing communication") without reciting an action that achieves that result. The specification does not clearly link any particular action to this recited step Part of the recited function is performed by the Remote Procedure Call Manager 732 software of Rights Operating System 602 that controls I/O controller 660 and Communications Controller 666. 2. The recited function is: creating and using a previously non-existent communications channel which is necessary and sufficient for exchanging information between the first device and a clearinghouse.
using said authorization information to gain access to or make at least one use of said first digital file	1. A user, process or device uses all of said authorization information in connection with executing VDE control(s) within VDE Secure Processing Environment(s) to gain access to or (as opposed to "and") make at least one use of the file received in the "receiving" step. Without using such authorization information, no access to or use of the file is allowed.
including using said key to decrypt at least a portion of said first digital file	1. The "at least one use of said digital file" must encompass decrypting at least a portion of the digital file using the key.
receiving a first control from said clearinghouse at said first device	1. This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites a step or result ("receiving") without reciting an action that achieves that result. The specification does not clearly link any particular action to this recited step. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b). 2. The recited function requires: obtaining a VDE secure container encapsulating a first control, authenticating the first device in accordance with VDE controls associated with the secure container, and accepting the secure container.
storing said first digital file	1. Storing in a memory of the first device, the entire digital file (as opposed to any incomplete portion thereof) received in the "receiving" step, by

Claim Phrase	Microsoft's Preliminary Construction
in a memory of said first device	executing VDE control(s) within VDE Secure Processing Environment(s).
using said first control to determine whether said first digital file may be copied and stored on a second device	1. Determining whether the first control, by itself, allows this particular first device to perform both of the following actions on this particular digital file: (1) copy it and (2) store it (as opposed to a copy of it) on a second device, by executing the first VDE control within VDE Secure Processing Environment(s). To the extent that either the copy or store action is not determined by this step to be permissible, that action is absolutely prohibited and incapable of occurring, and no user, process or device can perform it on this digital file.
if said first control allows at least a portion of said first digital file to be copied and stored on a second device	1. This "if" condition creates two branches for the recited process, each of which must be performed. Each time the "if" condition is met, all four of the later-recited actions (copying, transferring, storing, rendering) must occur. Each time it is not met, each of these four actions must be prohibited and incapable of occurring. 2. This "if" condition is met if and only if the first control allows any portion of the first digital file to be copied and also allows that same portion of the file (as opposed to the copy) to be stored on any second device. This "if" condition is based entirely on the first control and thus is met, as above, even if other VDE controls prohibit those actions. 3. This claim limitation's recitation of "first control allows at least a portion of said first digital file" is inconsistent with the claim limitation "whether said first digital file may be copied ... on a second device."
copying at least a portion of said first digital file	1. Copying at least some portion of the digital file (as opposed to a copy thereof), which portion may or may not be (or even include) the portion referred to in the claim limitation "if said first control allows at least a portion," by executing VDE control(s) within VDE Secure Processing Environment(s).
transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output	1. Transferring to some second device (which may or may not be the "second device" referred to in the claim limitation "if said first control allows at least a portion of said digital file to be copied and stored on a second device") at least some portion of the digital file (not a copy thereof), by executing VDE control(s) within VDE Secure Processing Environment(s). The transferred portion may or may not be (or even include) the portion referred to in the claim limitation "if said first control allows at least a portion," or the portion referred to the above limitation "copying at least a portion."
storing said first digital file portion	1. Storing the "at least a portion" which was transferred to the second device, of the digital file received in the "receiving" step (as opposed to a copy of the file).
'683:2	Claim as a Whole: The "system" is a VDE.
user controls	1. [This shall be construed as a disputed claim term.]
the first secure container having been received from a	1. The "first secure container" must identify the single apparatus from which it was received, and that apparatus must be different from the first apparatus. Alternatively, if the Court does not construe this claim language as requiring the "first secure container" to identify the single apparatus

Claim Phrase	Microsoft's Preliminary Construction
second apparatus	from which it was received: This claim language has no patentable weight. It recites a step taken in the creation of the recited system, not a structural or functional characteristic of the system. One studying a particular system (as opposed to the process by which it was created) to compare it to the claimed system, could not distinguish a secure container received from another apparatus from, e.g., a secure container created on the first apparatus, and thus could not determine whether this step was satisfied. 2. Receiving the secure container includes authenticating the intended recipient in accordance with VDE controls associated with the secure container. The first secure container may be received as bar codes in a fax transmission, or filled ovals on a form delivered through physical mail.
an aspect of access to or use of	1. Any one (as opposed to more than one) aspect of any access to or (as opposed to "and") use by any and all processes, users, and devices.
the first secure container rule having been received from a third apparatus different from said second apparatus	1. The "first secure container rule" must have been received encapsulated within a VDE secure container, and the intended recipient must have been authenticated in accordance with VDE controls associated with the secure container, and the "first secure container rule" must have been accepted by the first apparatus. The "first secure container rule" must identify the single apparatus from which it was received, and that apparatus must be different from the first apparatus. 2. Alternatively, if the Court does not construe this claim language as requiring the "first secure container" to identify the single apparatus from which it was received: This claim language has no patentable weight. It recites a step taken in the creation of the recited system, not a structural or functional characteristic of the system. One studying a particular system (as opposed to the process by which it was created) to compare it to the claimed system, could not distinguish a secure container rule received from another apparatus from, e.g., a secure container rule created on the first apparatus, and thus could not determine whether this step was satisfied.
hardware or software used for receiving and opening secure containers	1. This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites an undefined mechanism ("hardware or software") for performing a function (e.g., "opening") without reciting particular structure that performs that function. The specification does not clearly link any particular structure to this recited function. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b). 2. The recited function requires: the same single logical piece of either hardware or software (as opposed to both) must be capable of both receiving and opening secure containers, this "receiving" including authenticating the intended recipient in accordance with VDE controls associated with the secure container, and this "opening" performed by executing VDE control(s) within VDE Secure Processing Environment(s).
said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers	1. Each secure container which the "hardware or software used for receiving and opening secure containers" is capable of receiving and opening must have the capacity to contain a governed item, and must have associated with it (as opposed to any particular governed item) a secure container rule.

Claim Phrase	Microsoft's Preliminary Construction
protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus	1. A single VDE Secure Processing Environment, in addition to and not within the first apparatus, actively preventing (not merely being capable of preventing, and not merely resisting) any "user" of the first apparatus from tampering with any and all information encapsulated by the Secure Processing Environment (as opposed to tampering with the Secure Processing Environment itself). Other components may or may not provide part of this protecting function. 2. The protecting function is provided by use of the disclosed "component assembly" (VDE controls), "secure container," "protected processing environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "access control" "handcuffs" between specific "controls," specific "objects" (and their content at an arbitrary granular level), and specific "users."
hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container	1. This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites an undefined mechanism ("hardware or software") for performing a function ("applying … in combination") without reciting particular structure that performs that function. The specification does not clearly link any particular structure to this recited function. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b). 2. The recited function requires: a single logical piece of either hardware or software (as opposed to both) to apply the two separate rules in combination by assembling and executing a single control, and to govern any one or more aspects of any access or use by any process or user or device, of a governed item contained in a secure container (which may or may not be any "secure container" recited earlier). Other components may or may not provide part of the governing function. This "hardware or software" performs its functions by executing VDE control(s) within VDE Secure Processing Environment(s).
hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	1. This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites an undefined mechanism ("hardware or software") for performing a function (e.g., "transmission") without reciting particular structure that performs that function. The specification does not clearly link any particular structure to this recited function. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b). 2. The recited function requires: a single logical piece of either hardware or software (as opposed to both) is capable of both transmission and receipt of secure containers, this receipt including authenticating the intended recipient in accordance with VDE controls associated with the secure container. This "hardware or software" is separate from and in addition to the first apparatus, the recited protected processing environment, and the recited "hardware or software" used for receiving and opening secure containers." The transmission and receipt of the secure containers may be via bar codes in a fax transmission, or filled ovals on a form delivered through physical mail. This "hardware or software" performs its functions by executing VDE control(s) within VDE Secure Processing Environment(s).
'721:1	Claim as a Whole: The recited method is performed within a VDE.
digitally signing a first load module with a first digital signature designating the	1. Digitally signing a particular ("first") load module by using a first digital signature as the signature key, which signing indicates to any and all devices in the first device class that the signor authorized this load module for use by that device. No VDE device can perform any execution of any load module without such authorization. The method ensures that the load module cannot execute in a particular device class and ensures that no

Claim Phrase	Microsoft's Preliminary Construction
first load module for use by a first device class	device in that device class has the key(s) necessary to verify the digital signature.
digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class	1. Digitally signing a different ("second") load module by using a different ("second") digital signature as the signature key, which signing indicates to any and all devices in the second device class that the signor authorized this load module for use by that device. No VDE device can perform any execution of any load module without such authorization. The method ensures that the load module cannot execute in a particular device class and ensures that no device in that device class has the key(s) necessary to verify the digital signature. 2. All devices in the first device class have the same persistent (not just occasional) and identified level of tamper resistance and/or same persistent and identified level of security. All devices in the second device class have the same persistent and identified level of tamper resistance and/or same persistent and identified level of security. The identified level of tamper resistance and/or identified level of security for the first device class, is greater or less than the identified level of tamper resistance and/or identified level of security for the second device class.
distributing the first load module for use by at least one device in the first device class	1. The first load module, digitally signed as indicated above, is transmitted to at least one device in the first device class.
distributing the second load module for use by at least one device in the second device class	1. The second load module, digitally signed as indicated above, is transmitted to at least one device in the second device class.
"721:34	Claim as a Whole: The "protected processing environment" is part of and within VDE.
arrangement within the first tamper resistant barrier	1. The arrangement is located and executed wholly within the first tamper resistant barrier.
prevents the first secure execution space from executing the same executable accessed by a second secure execution	1. "A second secure execution space having a second tamper resistant barrier with a second security level different from the first security level": a second secure execution space (different from the first secure execution space) is part of the protected processing environment, and has a tamper resistant barrier (different from the first tamper resistant barrier) which has a persistent (not just occasional) security level greater or less than the first persistent security level.

Page 10 of 15

Claim Phrase	Microsoft's Preliminary Construction
space having a second tamper resistant barrier with a second security level different from the first security level	2. "The same executable accessed by": the same executable (as opposed to, e.g., two copies of the same executable) is simultaneously accessed by both the first secure execution space and the second secure execution space. 3. "Prevents the first secure execution space from executing": the arrangement prevents the first secure execution space, otherwise capable of executing the executable, from executing any part of the executable (e.g., on behalf of any user, process, or device).
'861:58	Claim as a Whole: The recited method is performed within a VDE.
creating a first secure container	1. This preamble language is a claim limitation. 2. Completely forming (as opposed to defining) a secure container within a VDE Secure Processing Environment(s).
including or addressing . . . organization information . . . desired organization of a content section . . . and metadata information at least in part specifying at least one step required or desired in creation of said first secure container	1. The same single descriptive data structure must either contain within its confines or address both organization information and metadata information. 2. Both the "desired" organization of the content section and also the "desired" step, occur after the descriptive data structure is accessed, not before. 3. The metadata information specifies a procedure, as opposed to a result or a data item.
at least in part determine specific information required to be included in said first secure container contents	1. The metadata information is used to determine the specific value, not merely the kind, of at least some of the information that must be placed inside the secure container. 2. The use of the metadata information actively requires the secure container creation steps to add this specific information to the first secure container, as opposed to the specific information being within the secure container for some other reason.
rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents	1. A rule designed for these particular secure container contents, which is used (by VDE control(s)) executing in VDE Secure Processing Environment(s)) to limit access to or use of at least a portion of the contents of the first secure container (by all users, processes, and devices). Without compliance with this rule, no process, user, or device is able to take the controlled access or use action.
'891:1	Claim as a Whole: The recited method is performed within a VDE.
resource processed in a secure operating	1. This preamble language is a claim limitation. 2. A component part of a first appliance's secure operating environment which is processed within that secure operating environment's special-

Claim Phrase	Microsoft's Preliminary Construction
environment at a first appliance	purpose Secure Processing Unit. A Secure Processing Unit is a special-purpose unit isolated from the rest of the world in which a hardware tamper-resistant barrier encapsulates a processor and internal secure memory. The barrier prevents all unauthorized interference, removal, observation, and use of the information and processes within it. The processor cryptographically verifies the integrity of all code loaded from the secure memory prior to execution, executes only the code that the processor has authenticated for its use, and is otherwise secure.
securely receiving a first entity's control at said first appliance	1. This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites a step or result ("securely receiving") without reciting an action that achieves that result. The specification does not clearly link any particular action to this recited step. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b).
	2. The recited function requires: A first appliance obtaining a VDE secure container encapsulating a control created, selected, or modified by a first entity, as part of a communication encrypted on the communications level, authenticating the first appliance in accordance with VDE controls associated with the secure container, and accepting the secure container.
securely receiving a second entity's control at said first appliance	1. This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites a step or result ("securely receiving") without reciting an action that achieves that result. The specification does not clearly link any particular action to this recited step. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b).
	2. The recited function requires: A first appliance obtaining a VDE secure container encapsulating a control created, selected, or modified by a second entity, as part of a communication encrypted on the communications level, authenticating the first appliance in accordance with VDE controls associated with the secure container, and accepting the secure container.
securely processing a data item at said first appliance, using at least one resource	1. Performing an operation, inside the special-purpose Secure Processing Unit of the first appliance, on a data item inside the Secure Processing Unit. The operation cannot be observed from outside the SPU and is performed only after the integrity of the program code for performing such operation is cryptographically verified. A Secure Processing Unit is a special-purpose unit isolated from the rest of the world in which a hardware tamper-resistant barrier encapsulates a processor and internal secure memory. The barrier prevents all unauthorized interference, removal, observation, and use of the information and processes within it. The processor cryptographically verifies the integrity of all code loaded from the secure memory prior to execution, executes only the code that the processor has authenticated for its use, and is otherwise secure.
securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item	1. Processing the resource (component part of a first appliance's secure operating environment) within the secure operating environment's special-purpose Secure Processing Unit to execute the first control and second control in combination within the SPU. This execution of these controls governs all use of the data item by all users, processes, and devices. The processing of the resource and execution of the controls cannot be observed from outside the SPU and is performed only after the integrity of the resource and controls is cryptographically verified. A Secure Processing Unit is a special-purpose unit isolated from the rest of the world in which a hardware tamper-resistant barrier encapsulates a processor and internal secure memory. The barrier prevents all unauthorized interference, removal, observation, and use of the information and processes within it. The processor cryptographically verifies the integrity of all code loaded from the secure memory prior to execution, executes only the code that the processor has authenticated for its use, and is otherwise secure.

Claim Phrase	Microsoft's Preliminary Construction
'900:155	**Claim as a Whole:** The "virtual distribution environment" is VDE.
first host processing environment comprising	1. A host processing environment that encompasses the recited computer hardware (central processing unit, main memory, and mass storage) and certain VDE Protected Processing Environment software loaded in that main memory and executing in that central processing unit, but does not encompass software, such as the recited tamper resistant software, which is stored in mass storage and not executing.
said mass storage storing tamper resistant software	1. The tamper resistant software is physically stored within, as opposed to being merely addressed by, the mass storage.
designed to be loaded into said main memory and executed by said central processing unit	1. The tamper resistant software is capable of being loaded into only said main memory and is capable of being executed only by said central processing unit.
said tamper resistant software comprising: . . . one or more storage locations storing said information	1. The tamper resistant software within said mass storage includes one or more storage locations within it. These storage locations are designated to store, and must store, information derived by the machine check programming, and must not store any other information.
derives information from one or more aspects of said host processing environment,	1. Deriving from the host processing environment hardware one or more values that uniquely and persistently identify the host processing environment and distinguish it from other host processing environments. 2. The "one or more aspects of said host processing environment" are distinguishing components or parts of the host processing environment itself, as opposed to, e.g., data or programs stored within the mass storage or main memory, or processes executing within the host processing environment.
one or more storage locations storing said information	1. One or more logical storage locations within the tamper resistant software storing only information derived by the machine check programming.
information previously stored in said one or more storage locations	1. Any information once stored in said "one of more storage locations storing said information," but not stored therein when the recited comparison occurs.
generates an indication based on the result of said comparison	1. Producing an indication based solely on the result of the "compares" step. There are only two possible indications: the comparison found an exact match, or it did not. The "indication" need not be displayed to a user.
programming which takes one or more actions based	1. Executable programming code that is a part of the tamper resistant software, when executed, and not a part of the host processing environment. Whenever the recited indication is generated, no matter what it indicates, this code (executing on the CPU for which it was designed

Claim Phrase	Microsoft's Preliminary Construction
on the state of said indication	and loaded in the memory for which it was designed) must take an action, or more than one action. The particular action(s) taken must be based solely on the state of that indication.
at least temporarily halting further processing	1. The action(s) taken by this programming must encompass halting or temporarily halting all further processing of the host processing environment and any processes running within it.
'912:8	**Claim as a Whole:** The recited method is performed within a VDE.
identifying at least one aspect of an execution space required for use and/or execution of the load module	1. Defining fully, without reference to any other information, at least one of the persistent features (aspects) of an execution space that are required for any use, and/or for any execution, of the load module. An execution space without all of those required aspects is incapable of making any such use (e.g., copying, displaying, printing) and/or execution of the load module.
said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security	1. The execution space Identifier, by itself, provides the load module with the capability of determining the persistent level of security of any execution space in which it is loaded, and of distinguishing between any two execution spaces based on their respective, determined persistent (not just occasional) "levels of security." This capability extends to at least two execution spaces providing a higher level of security and at least two execution spaces providing a lower level of security.
checking said record for validity prior to performing said executing step	Before executing any executable programming encompassed within any element which is directly or indirectly identified by any information contained within the first record, evaluating, within a VDE Secure Processing Environment, the values and formats of all data fields within the first record and confirming that they have legitimate values and formats.
'912:35	**Claim as a Whole:** The recited method is performed within a VDE.
received in a secure container	1. The first processing environment obtained a VDE secure container encapsulating the record inside, and authenticated the intended recipient in accordance with VDE controls associated with the secure container, and accepted the secure container.
said component assembly allowing access to or use of specified information	1. The component assembly identifies specific information over which it (by itself and with no other information), executing in a VDE Secure Processing Environment, allows access or use (as opposed to access "and" use). Unless allowed by the component assembly, no user, process, or device is able to access or use the specified information. The component assembly is associated with and dedicated to this particular specified information.
said first component	1. The first record by itself contains sufficient information to unambiguously identify the assembled component assembly, including all of its

Claim Phrase	Microsoft's Preliminary Construction
assembly specified by said first record	elements.
	2. This limitation is inconsistent with the recitation "first record containing identification information directly or indirectly identifying one or more elements of first component assembly."

Exhibit D

EXHIBIT D

Appended hereto, in accordance with Patent Local Rule 4-2(b), are copies of excerpts of dictionary definitions and other publications.

EXHIBIT D – MICROSOFT'S CORPORATION'S
PATENT LOCAL RULE 4-2 DISCLOSURE
(LIMITED TO "MINI-MARKMAN" CLAIMS),
CASE NO. C 01-1640 SBA

Exhibit D List of Dictionaries

No.	Dictionary
1	The New IEEE Standard Dictionary of Electrical and Electronic Terms (IEEE 100-1992), 1993, ISBN 1-55937-240-0
2	The Whole Internet: User's Guide and Catalog (O'Reilly & Associates, Inc) ISBN 1-56592-0252
3	Practical Unix Security (O'Reilly & Associates, Inc) ISBN 0-93717-5722
4	Computer Security Basics, Deborah Russell and G.T. Gangemi Sr. (O'Reilly & Associates, 1991) ISBN 0-93717-5714
5	Modern Methods for Computer Security and Privacy, Lance J. Hoffman (Prentice Hall, 1977) ISBN 0-13-595207-7
6	Distributed Systems, Second Edition, Sape Mullender (Addison Wesley, 1993) ISBN 0-20162-4273
7	Formal Models for Computer Security, Carl E Landwehr, ACM Computer Surveys, September 3, 1981 pg 247-275
8	Computer & Communications Security: Strategies for the 1990's, James Arlin Cooper
9	The Computer Security Handbook, Richard Baker (TAB Professional and Reference Books, 1985) ISBN 0-83060-3085
10	Computer Security Handbook 2nd Edition, Hutt, Bosworth, Hoyt (1987) ISBN 002915300X
11	National Information System Security (INFOSEC) Glossary, NSTISSI No. 4009, September 2000
12	Telecommunications: Glossary of Telecommunications Terms by Nation Communications Systems, 1996.
13	Internet Security Glossary, Network Working Group, RFC 2828, May 2000
14	Que's Computer User's Dictionary (1994) ISBN 1-56529-1255
15	The Dictionary of Computing and Digital Media: Terms and Acronyms, Brad Hansen (1999) ISBN 1-887902-38-4
16	Dictionary of Scientific and Technical Terms, 5th ed. (McGraw-Hill, 1994) ISBN 0-07-042333-4
17	The Computer Glossary: The Complete Illustrated Desk Reference, Alan Freedman (Computer Language Co., 1993) ISBN 0-8144-7801-8 (paperback) 0-8144-5104-7 (hardcover)
18	Prentice Hall's Illustrated Dictionary of Computing, 2nd Ed, Jonar C. Nader (Prentice Hall, 1992) ISBN 0-13205-7255
19	Computer Related Risks, Peter G. Neumann (1995) ISBN 0-201-55805-X

1

20	Dictionary of Computer Science, Engineering and Technology, Phillip A. Laplante (2001) ISBN 0-84932-6915
21	The American Heritage Dictionary of the English Language (1969) Standard Book Reference 0-395-09064-4 or 0-395-09065-2 or 0-395-09066-0
22	Webster's New World Dictionary of Computer Terms (1992) ISBN 0-671-84651-5
23	Webster's College Dictionary of Random House (1991) ISBN 0-679-40110-5 or 0-679-40100-8
24	Dictionary of Computing, Third Edition (Oxford, 1990) ISBN 0-19-853825-1
25	Funk & Wagnalls Standard College Dictionary, 1973
26	Newton's Telecom Dictionary, Harry Newton (1993) ISBN 0-93644-8422; (1996) ISBN 0-93644-8872
27	Tony Gunton, A Dictionary of Information Technology and Computer Science, Second Edition (NCC Blackwell Ltd 1993). ISBN 1-85554-327-3
28	Dictionary of Computer Science, Engineering and Technology, Phillip A. Laplante (2001) ISBN 0-84932-6915
29	Modern Operting Systems, Andrew S. Tanenbaum (Prentice Hall, 1992) ISBN 0-13588-1870
30	Unix System Security, Wood, Kochan (Hayden Books Unix System Library, 1985) ISBN 0-81046-2672
31	Microsoft Computer Dictionary (Microsoft Press, 1994) ISBN 1-55615-597-2
32	Microsoft Computer Dictionary, Third Edition (1997) ISBN 1-57231-446 –X Paperback
33	Security in Computing, Charles P. Pfleeger (Prentice Hall, 1989) 0-13798-9431
34	Information Security: Dictionary of Concepts, Standards and Terms, Dennis Longley, Michael Shain and William Caelli (Stockton Press, 1992) ISBN 1-56159-069-X or 0-333-54698-9
35	The Random House Dictionary of the English Language: College Edition, 1968
36	Dictionary of Object Technology: The Definitive Desk Reference, Donald G Firesmith and Edward M Eykholt (SIGS Book, 1995) ISBN 1-88484-2097
37	Webster's Ninth New Collegiate Dictionary, Merriam-Webster, 1987, ISBN 0-87779-508-8
38	Fundamentals of Database Systems, Ramez Elmasri and Shamkant B. Navathe (Benjamin/Dummings Publishing Company, 1989) ISBN 0-80530-1453
39	IBM Dictionary of Computing, George

	McDaniel (McGraw Hill, 1994) ISBN 0-07-031488-8 (hardcover) 0-07031-4896 (paperback)
40	Encyclopedia of Computer Science and Engineering, 2nd Edition (Van Nostrand Reinhold Company, 1983) ISBN 0-4423-24496-7

Exhibit E

EXHIBIT E – Production Documents

IN00004247	IN00029902	IN00075912	IN00075923	IN00075949
IN00075983	IN00075989	IN00076751	IN00076879	IN00076896
IN00076920	IN00078052	IN00171981	IN00172167	IN00173457
IN00173475	IN00173653	IN00173934	IN00174227	IN00174246
IN00174289	IN00174303	IN00174357	IN00174373	IN00174376
IN00174435	IN00174623	IN00174656	IN00174689	IN00174702
IN00174718	IN00174728	IN00174745	IN00174748	IN00174751
IN00174763	IN00174796	IN00174828	IN00174851	IN00174895
IN00174925	IN00174945	IN00174975	IN00175067	IN00175077
IN00175093	IN00175103	IN00175115	IN00175137	IN00175145
IN00175286	IN00175300	IN00175323	IN00175354	IN00175602
IN00175621	IN00175709	IN00175713	IN00175729	IN00175843
IN00176182	IN00176184	IN00176253	IN00176256	IN00176259
IN00176261	IN00176315	IN00176319	IN00176373	IN00176417
IN00176432	IN00176437	IN00176453	IN00176542	IN00176868
IN00176901	IN00177015	IN00177409	IN00177425	IN00177442
IN00177450	IN00177490	IN00177501	IN00177524	IN00177539
IN00177542	IN00178045	IN00178050	IN00178098	IN00178157
IN00178502	IN00178643	IN00178686	IN00179081	IN00179430
IN00179571	IN00179772	IN00182386	IN00182542	IN00182584
IN00182604	IN00182621	IN00182642	IN00182678	IN00182685
IN00182732	IN00182741	IN00182801	IN00182844	IN00182852
IN00182863	IN00182879	IN00182902	IN00183008	IN00183129
IN00183177	IN00183254	IN00183325	IN00183379	IN00183391
IN00183523	IN00183660	IN00183698	IN00183699	IN00183711
IN00183904	IN00183912	IN00183916	IN00183952	IN00183973
IN00183983	IN00184010	IN00184020	IN00184024	IN00184038
IN00184113	IN00184121	IN00184149	IN00184376	IN00184498
IN00184663	IN00184819	IN00184858	IN00184864	IN00185251
IN00185254	IN00185263	IN00185319	IN00185347	IN00185361
IN00186679	IN00186694	IN00186707	IN00186711	IN00186750
IN00186761	IN00186890	IN00187009	IN00187458	IN00189107
IN00189456	IN00189583	IN00189815	IN00189818	IN00189828
IN00510231	IN00515938	IN00520960	IN00521077	IN00521959
IN00525310	IN00529007	IN00532191	IN00532292	IN00790333
IN01104824	IN01105073	IN01274376	IN01275382	IN01275395
IN01275439	IN01275511	IT00000005	IT00000067	IT00000207
IT00000230	IT00000243	IT00000259	IT00000280	IT00000293
IT00000315	IT00000343	IT00000371	IT00000399	IT00000401
IT00000406	IT00000715	IT00000964	IT00001419	IT00001510
IT00001515	IT00001522	IT00001533	IT00001569	IT00001650
IT00001663	IT00001678	IT00001689	IT00001698	IT00001711
IT00001729	IT00001746	IT00001753	IT00001762	IT00001784
IT00001820	IT00001851	IT00001876	IT00001897	IT00001935
IT00001953	IT00001960	IT00001968	IT00001994	IT00002002
IT00002030	IT00002079	IT00002090	IT00002097	IT00002101
IT00002103	IT00002133	IT00002155	IT00002160	IT00002163

EXHIBIT E – MICROSOFT'S CORPORATION'S
PATENT LOCAL RULE 4-2 DISCLOSURE
(LIMITED TO "MINI-MARKMAN" CLAIMS),
CASE NO. C 01-1640 SBA

IT00002178	IT00002183	IT00002186	IT00002202	IT00002228
IT00002263	IT00002279	IT00002285	IT00002324	IT00002326
IT00002346	IT00002607	IT00002657	IT00002716	IT00002731
IT00002742	IT00002774	IT00002881	IT00002887	IT00003151
IT00003184	IT00003361	IT00003378	IT00003394	IT00003438
IT00003439	IT00003443	IT00003453	IT00003462	IT00003792
IT00003803	IT00003851	IT00003871	IT00003874	IT00004021
IT00004136	IT00004555	IT00004891	IT00004973	IT00004979
IT00004980	IT00004993	IT00005067	IT00005068	IT00005090
IT00005102	IT00005262	IT00005306	IT00005314	IT00005401
IT00005416	IT00005450	IT00005463	IT00005749	IT00006228
	IT00006425	IT00006666	IT00006977	IT00007422
IT00007789	IT00007992	IT00008109	IT00008235	IT00008285
IT00008360	IT00008467	IT00008479	IT00008555	IT00009310
IT00009829	IT00009847	IT00009922	IT00010328	IT00010428
IT00010486	IT00010632	IT00010655	IT00010875	IT00011180
IT00012629	IT00012853	IT00012969	IT00013156	IT00013520
IT00013557	IT00013564	IT00013569	IT00013604	IT00013624
IT00013657	IT00013666	IT00013667	IT00013715	IT00013750
IT00013765	IT00014049	IT00014707	IT00014488	IT00014514
IT00014521	IT00014525	IT00014533	IT00014590	IT00014690
IT00014707	IT00014785	IT00014850	IT00014871	IT00014879
IT00014940	IT00015007	IT00015191	IT00015210	IT00015230
IT00015234	IT00015237	IT00015260	IT00015273	IT00015284
IT00015288	IT00015292	IT00015667	IT00015891	IT00016296
IT00016479	IT00016854	IT00018144	IT00018217	IT00018281
IT00018305	IT00018770	IT00018841	IT00018879	IT00021839
IT00025971	IT00026603	IT00026662	IT00026722	IT00026782
IT00026903	IT00026970	IT00027106	IT00027113	IT00027255
IT00027264	IT00027271	IT00027531	IT00027539	IT00027879
IT00027898	IT00027900	IT00027927	IT00027943	IT00027960
IT00027974	IT00027989	IT00028003	IT00028116	IT00028128
IT00028227	IT00028234	IT00028249	IT00028254	IT00028290
IT00028292	IT00028304	IT00028336	IT00028371	IT00028528
IT00028627	IT00028641	IT00028660	IT00030738	IT00031303
IT00031329	IT00031344	IT00031364	IT00031375	IT00031385
IT00031395	IT00031410	IT00031438	IT00031446	IT00031490
IT00031513	IT00031532	IT00031560	IT00031572	IT00031586
IT00031604	IT00031624	IT00031643	IT00031930	IT00031938
IT00031982	IT00032016	IT00032268	IT00032370	IT00032436
IT00036848	IT00036849	IT00036850	IT00036851	IT00036852
IT00036853	IT00036854	IT00036855	IT00036856	IT00036857
IT00036858	IT00036859	IT00036860	IT00036861	IT00036862
IT00036863	IT00036864	IT00036865	IT00036866	IT00036867
IT00036868	IT00036869	IT00036870	IT00036871	IT00036872
IT00036873	IT00036874	IT00036875	IT00036876	IT00036877
IT00036878	IT00037270	IT00037296	IT00037303	IT00037307

EXHIBIT E – MICROSOFT'S CORPORATION'S
PATENT LOCAL RULE 4-2 DISCLOSURE
(LIMITED TO "MINI-MARKMAN" CLAIMS),
CASE NO. C 01-1640 SBA

EXHIBIT E – Production Documents

IT00037372	IT00037390	IT00037427	IT00037444	IT00037468
IT00037478	IT00037479	IT00037527	IT00037562	IT00037577
IT00038182	IT00038306	IT00038327	IT00038347	IT00038363
IT00038372	IT00038422	IT00038431	IT00038997	IT00039250
IT00039866	IT00040223	IT00040233	IT00040347	IT00040361
IT00040363	IT00041512	IT00041530	IT00042789	IT00045453
IT00045456	IT00045457	IT00045458	IT00046871	IT00049240
IT00050938	IT00050949	IT00050961	IT00051019	IT00051099
IT00051136	IT00051147	IT00051179	IT00051227	IT00051720
IT00051856	IT00051867	IT00051878	IT00051894	IT00051901
IT00051938	IT00051952	IT00052017	IT00052139	IT00052144
IT00052146	IT00052167	IT00052168	IT00054954	IT00055484
IT00069793	IT00095639	IT00095745	IT00095774	IT00095776
IT00095789	IT00095843	IT00095849	IT00095916	IT00095949
IT00096026	IT00096036	IT00096041	IT00096061	IT00096470
IT00096679	IT00096944	IT00097379	IT00097717	IT00113942
IT00114233	IT00114388	IT00114577	IT00114757	IT00117517
IT00117579	IT00117756	IT00117996	IT00118184	IT00118709
IT00118866	IT00119088	IT00119148	IT00119686	IT00119698
IT00119815	IT00119851	IT00119907	IT00119928	IT00120095
IT00120163	IT00120964	IT00121368	IT00121370	IT00121503
IT00122592	IT00124816	IT00124818	IT00124820	IT00124822
IT00124823	IT00124836	IT00124910	IT00124911	IT00124932
IT00124944	IT00125101	IT00125143	IT00125151	IT00125238
IT00125253	IT00125287	IT00132194	IT00132319	IT00132467
IT00132502	IT00132505	IT00132554	IT00132864	IT00133375
IT00133709	IT00134029	IT00134508	IT00135017	IT00135382
IT00136266	IT00136488	IT00136548	IT00137267	IT00138348
IT00138641	IT00139967	IT00140269	IT00140401	IT00141322
IT00142337	IT00143975	IT00149724	IT00150856	IT00167103
IT00169208	IT00177126	IT00188324	IT00191480	IT00192334
IT00197477	IT00197482	IT00197491	IT00210571	IT00214347
IT00247624	IT00340503	IT00383482	IT00399871	IT00399877
IT00421590	IT00516589	IT00523579	IT00523595	IT00523612
IT00523646	IT00523662	IT00523677	IT00523696	IT00523701
IT00543741	IT00550662	IT00559320	IT00560258	IT00565857
IT00566022	IT00698363	IT00698378	IT00698393	IT00698409
IT00702804	IT00702823	IT00702855	IT00702862	IT00702864
IT00702869	IT00702891	IT00702908	IT00702922	IT00702937
IT00702969	IT00702987	IT00703050	IT00703055	IT00703080
IT00703081	IT00703083	IT00703090	IT00703100	IT00703152
IT00703217	IT00703258	IT00703287	IT00703326	IT00703390
IT00703400	IT00703419	IT00703435	IT00703477	460MIC00007
460MIC00017	GNT00000001	GNT00004298	GNT00004304	GNT00004444
GNT00004851	GNT00004927	GNT00004958	LINN00001-709	NIST00001-2226
NSA 00275-3033	NV00000037	WW00143		

EXHIBIT E – MICROSOFT'S CORPORATION'S
PATENT LOCAL RULE 4-2 DISCLOSURE
(LIMITED TO "MINI-MARKMAN" CLAIMS),
CASE NO. C 01-1640 SBA

Exhibit F

EXHIBIT F - Publications

MSI0156840-45
MSI017361-62
MSI017548-556
MSI017864-70
MSI017899-911
MSI018529-74
MSI018811-19
MSI019082-99
MSI020348-370
MSI020373-384
MSI020389-396
MSI021744
MSI022371-380
MSI022440-455
MSI022766-23028
MSI027045-068
MSI036052-92
MSI036113-28
MSI067984-8007
MSI068022 et seq.
MSI079611-656
MSI079796-806
MSI079844-49
MSI079850-56
MSI079850-56
MSI080030-40
MSI080041-42
MSI080043-97
MSI080098-102
MSI080103-116
MSI080117-119
MSI080120-31
MSI080160-164
MSI080173-188
MSI080194-204
MSI080205-222
MSI080254-260
MSI080261-276
MSI080290-302
MSI080337-348
MSI080349-55
MSI080356-397
MSI080410-419
MSI080420-422

MSI080441-445
MSI080456-478
MSI080562-574
MSI080575-696
MSI080697-712
MSI080779-784
MSI080875-909
MSI080910-26
MSI080927-973
MSI080974-81007
MSI081052-66
MSI081140 et seq
MSI081240 et seq.
MSI081464 et seq.
MSI081464-717
MSI082792-826
MSI082958-3002
MSI083003-13
MSI083105-107
MSI083108-179
MSI083356 et seq.
MSI083356-99
MSI083400
MSI083410
MSI083423
MSI083423-443
MSI083444 et seq.
MSI085035-6
MSI085043-48
MSI085049-58
MSI085078-114
MSI085115-35
MSI085136-149
MSI085189-200
MSI085211
MSI085217-29
MSI085230-44
MSI085245-350
MSI085479-521
MSI085551-68
MSI085569
MSI085569-92
MSI085593-653
MSI085654

MSI085704 et seq.
MSI085756
MSI085831-33
MSI085834-36
MSI085837-39
MSI085840-42
MSI085843-44
MSI086146-55
MSI086641-52
MSI086653-62
MSI086675-86
MSI086687-703
MSI086704-727
MSI086845-863
MSI086864-67
MSI086893-904
MSI086905-919
MSI086923-25
MSI086926-32
MSI086946-950
MSI086951-73
MSI086985-87006
MSI087007-36
MSI087007-36
MSI087037-43
MSI087044-46
MSI087047-60
MSI087061-80
MSI087081-88
MSI087089-106
MSI087107-14
MSI087153-54
MSI087160-62
MSI087341-51
MSI087352-364
MSI087365-86
MSI087392-407
MSI087408-421
MSI087422-443
MSI087444-447
MSI087448-453
MSI087454-465
MSI087519-31
MSI087532-45

EXHIBIT F – MICROSOFT'S CORPORATION'S
PATENT LOCAL RULE 4-2 DISCLOSURE
(LIMITED TO "MINI-MARKMAN" CLAIMS),
CASE NO. C 01-1640 SBA

EXHIBIT F - Publications

MSI087558-75
MSI087576-85
MSI087586-592
MSI087598-623
MSI087681-693
MSI087694-707
MSI087717-24
MSI087725-36
MSI087737-47
MSI087748-64
MSI087765-75
MSI087776-793
MSI087811-820
MSI087821-838
MSI087839-51
MSI087852-65
MSI088177-79
MSI088186-203
MSI088297
MSI088297-313
MSI088314
MSI088342
MSI088363
MSI088368
MSI088508512
MSI088562-759
MSI088773-80
MSI088781-95
MSI088820-73
MSI088876-78
MSI088876-78
MSI088879-80
MSI088881-83
MSI088884-85
MSI088886-87
MSI088888-89
MSI088890-91
MSI088892-94
MSI088896-902
MSI088903-13
MSI088914-18
MSI088919-33
MSI088938-9026
MSI088953

MSI089068-165
MSI089191-200
MSI089974-90004
MSI090025-45
MSI090055-66
MSI090091-114
MSI090181-244
MSI093870-94277
MSI094278
MSI094738 et seq.
MSI095044 et seq.
MSI095787 et seq.
MSI096004 et seq.
MSI120670-720
MSI132777-87
MSI156788-93
MSI156834-39
MSI161724-31
MSI161742-52
MSI161753-60
MSI161761-96
MSI161797-800
MSI161856-65
MSI161886-94
MSI161895-901
MSI161921-42
MSI161943-68
MSI161969-85
MSI162040-60
MSI162061-75
MSI162132 et seq.
MSI162160-355
MSI162646
MSI162654-69
MSI162698-710
MSI162729-45
MSI162756-76
MSI162788-800
MSI162820-23
MSI162830-37
MSI162841-45
MSI163014-79
MSI163338-39
MSI163355-57

MSI163358-59
MSI163519-23
MSI163935-4204
MSI164205-4281
MSI164771-800
MSI164842-46
MSI168115-131
MSI168132-56
MSI168350-385
MSI173839-868
MSI173884-886
MSI173887-892
MSI173893-904
MSI173905-906
MSI175647-669
MSI175666-704
MSI175722-730
MSI17573-739
MSI175738-763
MSI175740-748
MSI175764-787
MSI175788-795
MSI175818-839
MSI175840-903
MSI175869-934
MSI175904-911
MSI175912-944
MSI175935-943
MSI175944-978
MSI176004-070
MSI176033-073
MSI176183-204
MSI192494-509
MSI192652-60
MSI192773-87
MSI197506-8536
MSI198537-8578
MSI198579-8690
MSI198691-8846
MSI199341
MSI199404
MSI199417
MSI199425
MSI199480

EXHIBIT F – MICROSOFT'S CORPORATION'S
PATENT LOCAL RULE 4-2 DISCLOSURE
(LIMITED TO "MINI-MARKMAN" CLAIMS),
CASE NO. C 01-1640 SBA

EXHIBIT F - Publications

MSI199485
MSI199525
MSI199536
MSI199550
MSI199576
MSI199605
MSI199612
MSI199618
MSI199633
MSI199645
MSI199681
MSI199700
MSI199736
MSI199738
MSI199743
MSI199755
MSI204966
MSI204983
MSI205081
MSI205118
MSI205137
MSI205190
MSI205529
MSI205548
MSI205621
MSI205633
MSI205648
MSI205650
MSI205659
MSI205660
MSI205749
MSI205967
MSI205981
MSI206028
MSI206144
MSI206178
MSI206672
MSI206764-76
MSI206777
MSI206951
MSI206952
MSI206982
MSI207089
MSI207745-80

MSI207781-819
MSI207820-46
MSI207847-72
MSI207873-901
MSI207998-8022
MSI208023-45
MSI208222-79
MSI208280-320
MSI208321-63
MSI208364-98
MSI208434-64
MSI208465-501
MSI208843-67
MSI209487-95
MSI209496-524
MSI209525-46
MSI209547-58
MSI209692-712
MSI209713-26
MSI209854-68
MSI209981-90
MSI210379-402
MSI210403-20
MSI210421-27
MSI210447
MSI210496-516
MSI210517-21
MSI210522-30
MSI210838-55
MSI210856-899
MSI210900-40
MSI210941-83
MSI210984-90
MSI211023-24
MSI211026-27
MSI211071-132
MSI211133-79
MSI211180-324
MSI211325-465
MSI211504-5
MSI211515-17
MSI211582-610
MSI213017-25
MSI213026-41

MSI213042-65
MSI213076-87
MSI213088-96
MSI213206-10
MSI213211-13
MSI213214-20

(see also cited production
documents such as LINN,
NIST)

EXHIBIT F – MICROSOFT'S CORPORATION'S
PATENT LOCAL RULE 4-2 DISCLOSURE
(LIMITED TO "MINI-MARKMAN" CLAIMS),
CASE NO. C 01-1640 SBA

Exhibit F Publications

Bates Number	Author and Title
MSI0156840	Willett, S., "Metered PCs: Is Your System Watching You?, Wave Systems Beta Tests New Technology," May 2, 1994.
MSI017361	Cox, B., "Superdistribution," January 1996.
MSI017548	Hauser, Ralf, C., "Does Licensing Require New Access Control Techniques?," August 12, 1993.
MSI017864	Purdy, G.B., et al., "A Software Protection Scheme," April 1982.
MSI017899	Sibert, O., et al., "The DigiBox: A Self-Protecting Container for Information Commerce," July 1995.
MSI018529	Lampson, B., et al. "Authentication in Distributed Systems in Theory and Practice," November 4, 1992.
MSI018811	Newman, B.C., "Proxy-Based Authorization and Accounting for Distributed Systems," 1993.
MSI019082	CUPID, "Protocols and Services (Version 1): An Architectural Overview," November 1997.
MSI020348	Herzberg, A., et al., "Public Protection of Software," November 1987.
MSI020373	Hot Java: "The Security Story," 1996
MSI020389	JavaSoft, "Frequently Asked Questions-Applet Security," June 7, 1996.
MSI021744	Arneke, D., "AT&T Encryption System Protects Information Services" News Release, January 9, 1995.
MSI022371	Low, S.H., et al., "Anonymous Credit Cards," November 1994.
MSI022440	Kristol, D.M., et al., "Anonymous Internet Mercentile Protocol," March 17, 1994.
MSI022766	The First USENIX Workshop on Electronic Commerce Proceedings, July 1995.
MSI027045	Denning, Dorothy E., et al., "Data Security," September 1979.
MSI036052	Wobber, E., et al. "Authenticating in the Taos Operating System," Digital Systems Research Center," December 10, 1993.
MSI036113	Olson, M., et al., "Concurrent Access Licensing," 1988.

Exhibit F Publications

MSI067984	Kahn, D., "The Codebreakers: The Story of Secret Writing," December 1996.
MSI068022	**Cohen, F.B., "Protection and Security on the Information Superhighway," 1995.**
MSI079611	**Brockschmidt, Kraig, "Inside OLE 2," 1994.**
MSI079796	Ioannidis, J., et al., "The Architecture and Implementation of Network-Layer Security Under Unix," October 1993.
MSI079844	Berners-Lee, T.J., et al., "Networked Information Services: The World-Wide Web," 1992.
MSI079850	Rivest, R.L., et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," 1978.
MSI079850	Rivest, R.L., et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," 1978.
MSI080030	Ferraiolo, D., et al., "Role-Based Access Control," 1992.
MSI080041	NIST, "Role Based Access Control," 1992.
MSI080043	U.S. Department of Commerce (NIST), "Security Requirements for Cryptographic Modules," undated.
MSI080098	Kreutzer, A.N., "An On-Line System for Controlling and Monitoring Software Usage in a Microcomputer Laboratory," August 1988.
MSI080103	**Millen, J.K., et al., "Security for Object-Oriented Database Systems," May 1992.**
MSI080117	Kim, L., et al., "Novell Cuisine," 1991.
MSI080120	**Koenig, A., "Automatic Software Distribution," June 1984.**
MSI080160	**Leiss, E., "On Authorization Systems with Grantor-Controlled Propagation on Privileges," 1983.**
MSI080173	**Strack, Hermann, "Extended Access Control in UNIX System V-ACLs and Context," August 1990.**
MSI080194	**Polk, T.W., "Approximating Clark-Wilson "Access Triples" with Basic UNIX Controls," October 1993.**
MSI080205	Kamens, J.I., "Retrofitting Network Security to Third-Party Applications-The SecureBase Experience," October 1993.

Exhibit F Publications

MSI080254	Gamble, Todd, "Implementing Execution Controls in Unix," 1993.
MSI080261	Epstein, J., "A Trusted X Window System Server for Trusted Mach," August 30, 1990.
MSI080290	Kelter, U., "Discretionary Access Controls in a High-Performance Object Management System," 1991.
MSI080337	Downs, D.D., et al., "Issues in Discretionary Access Control," April 1985.
MSI080349	Solomon, Daniel, J., "Processing Multilevel Secure Objects," April 1981.
MSI080356	Kim, Won, et al., "Object-Oriented Concepts, Databases, and Applications," 1989.
MSI080410	Maude, T., et al., "Hardware Protection Against Software Piracy," September 1984.
MSI080420	Lipson, S., "Little Black Box 'Blocks' Illicit Software Copying," September 14, 1986.
MSI080441	Sandhu, Ravi, S., et al., "Implementation Considerations for the Typed Access Matrix Model in a Distributed Environment," October 1992.
MSI080456	Rescorla, E., et al., "The Secure HyperText Transfer Protocol," June 1994.
MSI080562	Keefe, T.F., et al., "Prototyping the SODA Security Model," 1990.
MSI080575	National Security Agency, "A Guide to Understanding Security Modeling in Trusted Systems," October 1992.
MSI080697	Sandhu, R.S., "The Typed Access Matrix Model," May 1992.
MSI080779	Lunt, Teresa, "Multilevel Security for Object-Oriented Database Systems," 1990.
MSI080875	Tygar, J.D., et al., "Strongbox: A System for Self-Securing Programs," 1991.
MSI080910	Yee, B., et al., "Secure Coprocessors in Electronic Commerce Applications," July 1995.
MSI080927	Franklin, M., et al., "An Overview of Secure Distribution Computing," March 24, 1992.
MSI080974	Anderson, R., "Why Cryptosystems Fail," November 1993.
MSI081052	Bishop, M., "Anatomy of a Proactive Password Changer," 1992.

Exhibit F Publications

MSI081140	Time-Life Books, "Understanding Computers: Computer Security," 1986.
MSI081240	Wood, P.H., et al., "UNIX System Security," 1985.
MSI081464	Custer, Helen, "Inside Windows NT," 1993.
MSI081464	Custer, Helen, "Inside Windows NT," 1993.
MSI082792	Symantec Corporation, "THINK Pascal: The Fastest Way to Finished Software," 1990.
MSI082958	Olivier, M.S., et al., "A Taxonomy for Secure Object-Oriented Databases," 1994.
MSI083003	McCollum, C.J., et al., "Beyond the Pale of MAC and DAC-Defining New Forms of Access Control," 1990.
MSI083105	"Mach Books," viewed on February 6, 2002 at <http://www2.cs.cmu.edu/afs/cs/project/mach/public/www/doc/books.html.>
MSI083108	Department of Defense, "Trusted Computer System Evaluation Criteria," Dece,ber 1985.
MSI083356	LaLonde Wilf, R., et al., "Inside Smalltalk," Volume 1, 1990.
MSI083356	LaLonde Wilf, R., et al., "Inside Smalltalk," Volume 1, 1990.
MSI083400	Muftic, Sead, "Security Mechanisms for Computer Networks," 1989.
MSI083410	Konheim, Alan, G., et al.,"Cryptography: A Primer," 1981.
MSI083423	Davies, D.W., et al., "Security for Computer Networks," 1984.
MSI083423	Davies, D.W., et al., "Security for Computer Networks," 1984.
MSI083444	Castano, S., et al., "Database Security," 1995.
MSI085035	OOPSLA 1993: Addendum to the Proceedings, "Security for Object-Oriented Systems," September 26-October 1, 1993.
MSI085043	Thuraisingham, B., et al., "Parallel Processing and Trusted Database Management Systems," 1993.
MSI085049	Secure Computing, "Constructing a High Assurance Mail Guard," 1994.
MSI085078	Sandhu, R.S., et al., "Data and Database Security and Controls," 1993.

Exhibit F Publications

MSI085115	Thomas, R.K., et al., "Implementing the Message Filter Object-Oriented Security Model without Trusted Subjects," August 1992.
MSI085136	Sandhu, R., et al., "A Secure Kernelized Architecture for Multilevel Object-Oriented Databases," June 1991.
MSI085189	Sibert, O., et al., "The Intel 80x86 Processor Architecture: Pitfalls for Secure Systems," May 1995.
MSI085211	Ware, W., Chairman RAND Corporation "Panel: The InterTrust Commerce Architecture," 1997.
MSI085217	Fine, T.,et al, "Assuring Distributed Trusted Mach," 1993.
MSI085230	Minear, S.E., "Providing Policy Control Over Object Operations in a Mach Based System," April 28, 1995.
MSI085245	Harris, J., et al., "Bento Specification," July 15, 1993.
MSI085479	Young, W.D., "Verifiable Computer Security and Hardware: Issues," September 1991.
MSI085551	Denning, A., "OLE Controls Inside Out," 1995.
MSI085569	Denning, D., "Crytography and Data Security," 1982.
MSI085569	Denning, D., "Crytography and Data Security," 1982.
MSI085593	Schneier, Bruce, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," 1994.
MSI085654	Garfinkel, Simson, et al., "Practical UNIX Security," 1991.
MSI085704	Dougherty, D., et al., "The Mosaic Handbook for the X Window System," 1994.
MSI085756	Curry, D.A., "UNIX System Security: A Guide for Users and System Administrators," 1992.
MSI085831	International Infrastructure Standards Panel, "IISP Need #31-Containers or Secure Packaging," September 18, 1995.
MSI085834	International Infrastructure Standards Panel, "IISP Need #32-Authentication of Content," September 18, 1995.
MSI085837	International Infrastructure Standards Panel, "IISP Need #33-Control Enforcement," September 18, 1995.

Exhibit F Publications

MSI085840	International Infrastructure Standards Panel, "IISP Need #34-Billing and Payment," September 18, 1995
MSI085843	International Infrastructure Standards Panel, "IISP Need #35-Reporting," September 18, 1995.
MSI086146	Kaplan, M., "IBM Cryptolopes, Super Distribution and Digital Rights Management," December 30, 1996.
MSI086641	Sebes, E.J., et al., "The Triad System: The Design of a Distributed, Real-Time, Trusted System," January 22, 1998.
MSI086653	Sebes, E.J., et al., "The Architecture of Triad: A Distributed, Real-Time, Trusted System," (undated).
MSI086675	Sebes, E.J., "Overview of the Architecture of Distributed Trusted Mach," undated.
MSI086687	Vickers Benzel, T.C., et al., "Identification of Subjects and Objects in a Trusted Extensible Client Server Architecture," undated.
MSI086704	Borenstein, N., "MIME Extensions for Mail-Enabled Applications: Application/Safe-Tel and Multipart/Enabled-Mail," November 1993.
MSI086845	Bellare, M., "iKP-A Family of Secure Electronic Payment Protocols," April 16, 1995.
MSI086864	**Harn, Lein, et al., "A Software Authentication System for the Prevention of Computer Viruses," 1992.**
MSI086893	Deutsch, P., "GZIP File Format Specification Version 4.3," May 1996.
MSI086905	**Gong, Li, "A Secure Identity-Based Capability System," January 1989.**
MSI086923	Merkle, R.C., "Secure Communications Over Insecure Channels," April 1978.
MSI086926	Denning, D.E., "Secure Personal Computing in an Insecure Network," August 1979.
MSI086946	**Medvinsky, G., et al., "NetCash: A Design for Practical Electronic Currency on the Internet," 1993.**
MSI086951	Franz, M., "Technological Steps Toward a Software Component Industry," undated.
MSI086985	Kent, S., et al., "Privacy Enhancement for Internet Electronic Mail: Part II--Certificate-Based Key Management," August 1989.

Exhibit F Publications

MSI087007	Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part I-- Message Encipherment and Authentication Procedures," August 1989.
MSI087007	Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part I-- Message Encipherment and Authentication Procedures," August 1989.
MSI087037	**Chaum, D., "Achieving Electronic Privacy," August 1992.**
MSI087044	Microsoft Press, OLE 2 Programmer's Reference; Volume 1, "Working with Windows Objects," 1994.
MSI087047	**Brockschmidt, K., "A Primer on Designing Custom Controls," March/April 1992.**
MSI087061	Klemond, P., "Taking the Bull by the Horns: Investigating Object Linking and Embedding, Part I," March/April 1992.
MSI087081	Klemond, P., "Investigating Object Linking and Embedding, Part II: Adding Server Support," May/June 1992.
MSI087089	**DiLascia, Paul, "OLE Made Almost Easy: Creating Containers and Servers Using MFC 2.5," April 1994.**
MSI087107	**Coad, Peter, "Object-Oriented Patterns," September 1992.**
MSI087153	Zelnick, Nate, "Keeping Business Safe on the Internet," April 25, 1995.
MSI087160	**Lucent Technologies, "AT&T Encryption System Protects Information Services," January 9, 1995.**
MSI087341	**Birrell, Andrew, D., et al., "A Global Authentication Service Without Global Trust," April 1986.**
MSI087352	Gasser, M., et al., "The Digital Distributed System Security Architecture," 1989.
MSI087365	**Abadi, M., et al., "Authentication and Delegation with Smart-Cards," 1990.**
MSI087392	Zeleznick, M.P., "Security Design in Distributed Computing Applications," December 1993.
MSI087408	**Moffett, Jonathan, D., et al., "An Introduction to Security Distributed Systems," August 1993.**
MSI087422	Netscape, "SSL 2.0 Protocol Specification," February 9, 1995.

Exhibit F Publications

MSI087444	Davis, D., et al., "Network Security via Private-Key Certificates," October 1990.
MSI087448	Gruber, R., et al., "Disconnected Operation in the Thor Object-Oriented Database System," December 1994.
MSI087454	Ting, T.C., et al., "Requirements, Capabilities and Functionalities of User Role Based Security for an Object-Oriented Design Model," 1992.
MSI087519	Gifford, David, K., "Crytographic Sealing for Information Secrecy and Authentication," 1982.
MSI087532	Boly, J.P., et al., "The ESPIRIT Project CAFÉ: High Security Digital Payment Systems," 1994.
MSI087558	Kluepfel, H.M., "Securing a Global Village and its Resources: Baseline Security for Interconnected Signaling System #7 Telecommunications Networks," 1993.
MSI087576	Uhler, Stephen A., "PhoneStation, Moving the Telephone onto the Virtual Desktop," January 1993.
MSI087586	Brown, Patrick W., "Digital Signatures: Can They Be Accepted as Legal Signatures in EDI?," November 1993.
MSI087598	Popek, Gerald, J., et al., "Encryption and Secure Computer Networks," December 1979.
MSI087681	Picciotto, J., et al., "Extended Labeling Policies for Enhanced Application Support," 1994.
MSI087694	Born, E, et al., "Discretionary Access Control by Means of Usage Conditions," 1994.
MSI087717	Russell, S., "Paradigms for Verification of Authorization at Source of Electronic Documents in an Integrated Environment," 1993.
MSI087725	Olivier, M.S., et al., "Building a Secure Database Using Self-Protecting Objects," 1992.
MSI087737	Press, J., "Secure Transfer of Identity and Privilege Attributes in an Open Systems Environment," 1991.
MSI087748	Fugini, M.G., et al., "Authorization and Access Control in the Office-Net System," 1989.
MSI087765	Hardjono, Thomas, "Record Encryption in Distributed Databases," January 1990.

Exhibit F Publications

MSI087776	Calas, C., "Distributed File System Over a Multilevel Secure Architecture Problems and Solutions," 1994.
MSI087811	**Russell, S., "Planning for the EDI of Tomorrow Using Electronic Document Authorization," 1993.**
MSI087821	Lin, P., "The Encapsulated Security Services Interface (ESSI)," 1993.
MSI087839	**Fugini, M., et al., "Security Management in Office Information Systems," 1984.**
MSI087852	Montini, G, et al., "Access Control Models and Office Structures," 1984.
MSI088177	Multics, Home; viewed on November 12, 2001 at <http://www.multicians.org>.
MSI088186	Corbato, F.J., et al., "Introduction and Overview of the Multics System," 1992.
MSI088297	Moffett, J., et al., "Specifying Discretionary Access Control Policy for Distributed Systems," September 18, 1990.
MSI088297	Moffett, J., et al., "Specifying Discretionary Access Control Policy for Distributed Systems," September 18, 1990.
MSI088314	Moffett, J.D., "Specification of Management Policies and Discretionary Access Control," June 28, 1994.
MSI088342	Moffett, J.D., "Specification of Management Policies and Discretionary Access Control," 1994.
MSI088363	Moffett, J.D.,et al., "Policy Hierarchies for Distributed Systems Management," December 1993.
MSI088368	Moffett, J.D., et al., "The Representation of Policies as System Objects," November 1991.
MSI088508	Lampson, B.W., "A Note on the Confinement Problem," 1973.
MSI088562	**Olivier, M.S., "Secure Object-Oriented Databases," December 1991.**
MSI088773	Thuraisingham, M.B., "Mandatory Security in Object-Oriented Database Systems," October 1989.
MSI088781	**Chaum, D., "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," October 1985.**
MSI088820	**Lampson, B., "Computer Security," 1991.**

Exhibit F Publications

MSI088876	Walker, S., "Notes from RSA Data Security Conference," January 18, 1994.
MSI088876	Walker, S., "Notes from RSA Data Security Conference," January 18, 1994.
MSI088879	RSA Security; News; <http://rsasecurity.com/news/pr/9401.html.>, dated January 12, 1994.
MSI088881	RSA Security; News; "iPower's Data Security Approach," <http://rsasecurity.com/news/pr/940112-10.html.>, dated January 12, 1994.
MSI088884	RSA Security; News; "General Magic Picks RSA," <http://rsasecurity.com/news/pr/940112-3.html.>, dated January 12, 1994.
MSI088886	RSA Security; News; "Enterprise Solutions Announces RSA Mail," <http://rsasecurity.com/news/pr/940112-2.html.>, dated January 12, 1994.
MSI088888	RSA Security; News; "Hewlett-Packard Chooses RSA," <http://rsasecurity.com/news/pr/940112-5.html.>, dated January 12, 1994.
MSI088890	RSA Security; News; "Hilgraeve Ships Secure Version of HyperACCESS/5," <http://rsasecurity.com/news/pr/940112-8.html.>, dated January 12, 1994.
MSI088892	RSA Security; News; "RSA Enters Wireless Arena," <http://rsasecurity.com/news/pr/940112-6.html.>, dated January 12, 1994.
MSI088896	Williams, S., "An MSJ Interview with Microsoft's Chief Architect of OLE, Tony Williams," October 1993.
MSI088903	Brockschmidt, K., "OLE 2.0 Part II: Implementing a Simple Windows Object Using Either C or C++," October 1993.
MSI088914	Brockschmidt, K., "Introducing OLE 2.0, Part 1: Windows Objects and the Component Object Model," August 1993.
MSI088919	Brockschmidt, K., "Implementing OLE 2.0, Part III: Uniform Data Transfer with Data Objects," December 1993.
MSI088938	Townsend, J.E., "NIST on Internet Security," March 22, 1994.
MSI088953	Curry, David A., "Improving the Security of Your Unix System," April 1990.
MSI089068	Kohl, J., "The Kerberos Network Authentication Services (V5)," September 1993.

Exhibit F Publications

MSI089191	Bertino, Elisa, "Data Hiding and Security in Object-Oriented Databases," 1992.
MSI089974	Kim, W., et al., "Features of the ORION Object-Oriented Database System," 1989.
MSI090025	Kelter, U., et al., "Type Level Access Controls for Distributed Structurally Object-Oriented Database Systems," November 1992.
MSI090055	Wong, R., et al., "The SIDOS System: A Secure Distributed Operating System Prototype," October 1989.
MSI090091	OMG Security Working Group, "OMG White Paper on Security," April 1994.
MSI090181	National Computer Security Center, "Trusted Unix Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX (R) System," August 18, 1989.
MSI093870	UNKNOWN
MSI094278	**UNKNOWN**
MSI094738	**UNKNOWN**
MSI095044	Tanenbaum, A.S., "Operating Systems: Design and Implementation," 1987.
MSI095787	Date, C.J., "An Introduction to Database Systems," 4th. Ed., Vol. 1, 1987.
MSI096004	Tanenbaum, A.S., "Modern Operating Systems," 1992.
MSI120670	UNKNOWN
MSI132777	E-mail from Caglar Gunyakti entitled: "Private Test Needed," April 28, 2001.
MSI156788	**Clark, Paul, C., et al., "BITS: A Smartcard Protected Operating System," November 1994.**
MSI156834	**O'Connor, MaryAnn, "New Distribution Option for Electronic Publishers," March 1994.**
MSI161724	**Blaze, Matt, "A Crytographic File System for Unix," November 1993.**
MSI161742	Ferraiolo, D., et al., "Role-Based Access Control," 1992.
MSI161753	Hardy, N., "The Keykos Architecture," December 1990.
MSI161761	Miller, S.P., et al., "Kerberos Authentication and Authorization System," October 27, 1998.

Exhibit F Publications

	October 27, 1998.
MSI161797	IBM, "OpenDoc vs. OLE 2.0: Superior by Design," January 1994.
MSI161856	Brickell, E.F., et al., "The SKIPJACK Algorithm," July 28, 1993.
MSI161886	Blaze, M., "Key Management in an Encrypting File System," 1994.
MSI161895	**Woo, Thomas, Y.C., et al., "A Framework for Distributed Authorization," November 1993.**
MSI161921	Davin, J., et al., "SNMP Administrative Model," July 1992.
MSI161943	**Galvin, J., et al., "SNMP Security Protocols," July 1992.**
MSI161969	McCloghrie, K., et al., "Definitions of Managed Objects for Administration of SNMP Parties," July 1992.
MSI162040	Case, J., "A Simple Network Management Protocol (SNMP)," May 1990.
MSI162061	Information Systems Audit and Control Association-Montreal Chaper, "Authentification dans les environnements de traitement distributes," undated.
MSI162132	**Meyer, C.H., et al., "Cryptography: A New Dimension in Computer Data Security," 1982.**
MSI162160	Hewlett Packard Co., "Manager's Guide to MPE/iX Security," April 1994.
MSI162646	Hansen, S.E., et al., "Automated System Monitoring and Notification with Swatch," November 1993.
MSI162654	Bellovin, S.M., "There Be Dragons," August 15, 1992.
MSI162698	Bellovin, S.M., "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," May 1992.
MSI162729	Brands, S., "Untraceable Off-line Cash in Wallets with Observers," 1993.
MSI162756	White, J.E., "Telescript: The Foundation for the Electronic Marketplace," November 30, 1993.
MSI162788	White, J.E., "Telescript Technology: An Introduction to the Language," 1994.
MSI162820	Johnson, R., "Info on Telescript," December 6, 1994.

Exhibit F Publications

MSI162830	"An Introduction to Safety and Security in Telescript," undated.
MSI162841	Gosling, J., "Oak Intermediate Bytecodes," 1995.
MSI163014	Kohl, J., et al, "The Kerberos Network Authentication Service," June 30, 1991.
MSI163338	"A Brief History of the Green Project," viewed on March 12, 2002 at <http://java.sun.com/people/jag/green/index.html>.
MSI163355	IBM,"IBM Cryptolope Technology-Executive Summary," viewed on March 13, 2002 at <http://www-3.ibm.com/software/security/cryptolope.about.html>.
MSI163358	IBM, "Key Cryptolope Components," viewed on March 13, 2002 at <http://www-3.ibm.com/software/security/cryptolope.about.html>.
MSI163519	Stubblebine, S.G., "Security Services for Multimedia Conferencing," September , 1993.
MSI163935	NIST & NSA, "Federal Criteria Information Technology Security," Vol. II, Version 1.0, December 1992.
MSI164205	Rashid, R.F., "CMU Computer Science: A 25th Anniversary Commemorative," 1991.
MSI164771	**Multics History, visited on October 8, 1991 at <http://www.multicians.org/history.html>.**
MSI164842	**Halfhill, Tom, R., et al., "Just Like Magic?," February 1994.**
MSI168115	Chaum, D., et al., "Wallet Databases with Observers," 1998.
MSI168132	**Walker, Bruce, J., et al., "Computer Security and Protection Structures," 1977.**
MSI168350	Stallings, W., "Cryptography and Network Security: Principles and Practice," 1999.
MSI173839	Levine, P.H., et al., "Apollo Network License Server," October 1987.
MSI173884	Cabell, D., et al., "Software Protection," May 1985.
MSI173887	Glatzer, H., "The Promise of LANs MIS Back in Control," March 1985.
MSI173893	Cook, S., "Net Results," December 1985.
MSI173905	Kramer, M., "Strength in Numbers," July 22, 1986.

Exhibit F Publications

MSI175647	Custer, H., "Inside the Windows NT File System," 1994.
MSI175666	Appendix for Custer, H., "Inside the Windows NT File System," 1994.
MSI175722	Index for Custer, H., "Inside the Windows NT File System," 1994.
MSI17573	Solomon, A., "PC Viruses: Detection, Analysis and Cure," November 1991.
MSI175738	Glossary for Solomon, A., "PC Viruses: Detection, Analysis and Cure," November 1991.
MSI175740	Roberts, R., et al., Compute!'s "Computer Security," 1989.
MSI175764	Bibliography for Shaffer, S.L., et al., "Network Security," 1994.
MSI175788	Contents for Denning, P.J., "Computers Under Attack; Intruders, Worms & Viruses," 1990.
MSI175818	Keyword Index for Horster, P., "Communications and Multimedia Security II," 1996.
MSI175840	Index for Park, J.S., "AS/400 Security in a Client/Server Environment," 1995.
MSI175869	Diffie, et al., "Privacy on the Line: The Politics of Wiretapping and Encryption," 1998.
MSI175904	Bibliography for Diffie, et al., "Privacy on the Line: The Politics of Wiretapping and Encryption," 1998.
MSI175912	Index for Diffie, et al., "Privacy on the Line: The Politics of Wiretapping and Encryption," 1998.
MSI175935	Baker, R.H., "The Computer Security Handbook," 1985.
MSI175944	Hoffman, L.J., "Modern Methods for Computer Security and Privacy," 1977.
MSI176004	Krol, E., "The Whole Internet User's Guide and Catalog," 2nd. Ed., 1992.
MSI176033	Glossary for Krol, E., "The Whole Internet User's Guide and Catalog," 2nd. Ed., 1992.
MSI176183	Holsinger, E., "How Music and Computers Work," 1994.
MSI192494	**Bell-Labs Secure Technologies, "Information Vending Encryption System (IVES)™," May 31, 2002.**
MSI192652	Rubin, A.D., "Trusted Distribution of Software Over the Internet," 1995.

Exhibit F Publications

MSI192773	Kohl, J.T., et al., "The Evolution of the Kerberos Authentication Service," undated.
MSI197506	CardTech/SecurTech 94 Conference Proceedings, "Building Foundations for Innovation," April 1994.
MSI198537	Smart Card 1993 Conference Proceedings, "Day 1: Communications and Marketing Systems & Market Overview," 1993.
MSI198579	Chaum, D., "Smart Card 2000," 1991.
MSI198691	Global Projects Group, "Smart Card Technology International: The Global Journal of Advanced Card Technology," undated.
MSI199341	Vittal, J., "Active Message Processing: Messages as Messengers," 1980.
MSI199404	Chaum, D., "Achieving Electronic Privacy," August 1992.
MSI199417	Chaum, D., "Untraceable Electronic Cash," Extended Abstract, 1988.
MSI199425	Schaumüller-Bichl, S., "IC-Cards in High-Security Applications," undated.
MSI199480	Medvinsky, G., et al., "NetCash: A Design for Practical Electronic Currency on the Internet," 1993.
MSI199485	Dukach, S., "SNPP: A Simple Network Payment Protocol," December 1992.
MSI199525	Gifford, D., et al., "The Cirrus Banking Network," August 1985.
MSI199536	National Semiconductor "iPower Technology," undated.
MSI199550	Abadi, M., et al., "Authentication and Delegation with Smart-Cards," October 22, 1990, revised July 30, 1992.
MSI199576	Carnegie Mellon University, "Internet Billing Server," Prototype Scope Document, INI Tech Report, October 14, 1993.
MSI199605	Krajewski, Jr., M., et al., Concept for a Smart Card Kerberos," 1992.
MSI199612	Krajewski, Jr., M., "Smart Card Augmentation of Kerberos," February 1993.
MSI199618	Krahewsjum Jr., M., "Applicability of Smart Cards to Network User Authentication," 1994.
MSI199633	Harty, K., et al., "Case Study: The VISA Transaction Processing System," undated.

Exhibit F Publications

MSI199645	International Standard, "Bank Card Originated Messages: Interchange Message Specification Content for Financial Transactions," August 15, 1987.
MSI199681	Rivest, R., "The MD5 Message-Digest Algorithm," April 1992.
MSI199700	Voydock, V.L., et al., "Security Mechanisms in High-Level Network Protocols," June 1983.
MSI199736	Needham, R.M., "Ading Capability Access to Conventional File Servers," January 1979.
MSI199738	Gligor, V.D., et al., "Object Migration and Authentication," November 1979.
MSI199743	Chaum, D.L., et al., "Implementing Capability-Based Protection Using Encryption," July 17, 1978.
MSI199755	Gifford, D.K., "Cryptographic Sealing for Information Secrecy and Authentication," April 1982.
MSI204966	Johnson, H.L., et al., "A Secure Distributed Capability Based System," 1985.
MSI204983	Tanenbaum, A.S., et al., "Distributed Operating Systems," December 1985.
MSI205081	Voydock, V.L., et al., "Security Mechanisms in High-Level Network Protocols," June 1983.
MSI205118	Rushby, J.M., "Design and Verification of Secure Systems," 1981.
MSI205137	Clark, P.C., et al., "BITS: A Smartcard Protected Operating System," November 1994.
MSI205190	Brumm, P., et al., "80386/80486 Assembly Language Programming," 1993.
MSI205529	Hutt, A.E., et al., "Computer Security Handbook," 1988.
MSI205548	Brown, C.W., "Security for Minicomputers and Microcomputers," (undated).
MSI205621	The Risks Digest, "Forum on Risks to the Public in Computers and Related Systems," Vol. 15; Issue 39, January 21, 1994
MSI205633	The Risks Digest, "Forum on Risks to the Public in Computers and Related Systems," Vol. 15; Issue 47, February 9, 1994.
MSI205648	Halfhill, T.R., et al., "Agents on the Loose," February 1994.
MSI205650	Wayner, P., "Agents Away," May 1994.

Exhibit F Publications

MSI205659	Hawk, H.S., "RSA & General Magic," email to Good Guys, January 6, 1994.
MSI205660	Byte.com, "Speaking the Same Language," May 1994.
MSI205749	Atkins, D., et al., "The Magic Words are Squeamish Ossifrage," (undated).
MSI205967	Schill, A., et al., "Mobility Aware Multimedia X. 400 e-mail: A Sample Application Based on a Support Platform for Distributed Mobile Computing," undated.
MSI205981	National Institute of Standards and Technology, "History of Computer Security: Early Computer Security Papers, Part 1," 1998.
MSI206028	Department of Defense Standard, "Department of Defense Trusted Computer System Evaluation Criteria," December 1985.
MSI206144	Department of Defense Computer Security Center, "Department of Defense Password Management Guideline," April 12, 1985.
MSI206178	"Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments," http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-004-85.html, June 25, 1985.
MSI206672	Forcht, K.A., "Computer Security Management," 1994.
MSI206764	Olivier, M.S., et al., "DISCO: A Discretionary Security Model for Object-Oriented Databases," 1992.
MSI206777	Olivier, M.S., "A Multilevel Secure Federated Database," 1994.
MSI206951	"iOpener," Registered Trademark of National Semiconductor Corporation, Registration date October 4, 1994.
MSI206952	U.S. Patent and Trademark Coversheet for National Semiconductor Corporation "iOpener" Trademark, Registration date October 4, 1994.
MSI206982	UNKNOWN
MSI207089	Leary, P., "Are There Ciphers in Shakespeare?," 1995.
MSI207745	Toohey, J., "Using OLE 2.X in Application Development," 1994
MSI207781	Holzner, S., "Heavy Metal OLE 2.0 Programming," 1994.
MSI207820	Sheridan Software Systems, "Data Widgets 2.0: OLE Controls for Database Application Development," 1993-1995.

Exhibit F Publications

MSI207847	van Gilluwe, F., "The Undocumented PC: A Programmer's Guide to I/O, Cpus, and Fixed Memory Areas," 1994.
MSI207873	Short, K.L., "Microprocessors and Programmed Logic," 1981.
MSI207998	Table of Contents: Motorola MC68030 User's Manual, undated.
MSI208023	Mullender, S., "Distributed Systems," 1989.
MSI208222	Orfali, R., et al., "The Essential Distributed Objects Survival Guide," 1996.
MSI208280	Lockhart, Jr., H.W., "OSF DCE Guide to Developing Distributed Applications," 1994.
MSI208321	Open Software Foundation, "OSF DCE Administration Guide-Core Components," 1993.
MSI208364	Rosenberry, W., et al., "Distributing Applications Across DCE and Windows NT," 1993.
MSI208434	Shirley, J., "Guide to Writing DCE Applications," 1st Ed. 1992.
MSI208465	Shirley, J., et al., "Guide to Writing DCE Applications," 2nd Ed. 1994.
MSI208843	Honeyman, P., "Digest of the First UNSENIX Workshop on Electronic Commerce (EC 95)," July 1995.
MSI209487	Rubin, A.D., "Trusted Distribution of Software Over the Internet," 1995.
MSI209496	Tanenbaum, A.S., et al., "Experiences with the Amoeba Distributed Operating System," 1990.
MSI209525	Tanenbaum, A.S., et al., "The Amoeba Distributed Operating System-A Status Report," 1991.
MSI209547	Tanenbaum, A.S., et al., "The Amoeba Distributed Operating System," 1990.
MSI209692	Kim, G.H., et al., "The Design and Implementation of Tripwire: A File System Integrity Checker," November 19, 1993.
MSI209713	Farmer, D., "The COPS Security Checker System," July 10, 1992.
MSI209854	Kohl, J.T., et al., "The Evolution of the Kerberos Authentication System," 1991.
MSI209981	Lewontin, S., et al., "The DCE Web Project: Providing Authorization and Other Distributed Services to the World Wide Web," February 22, 2002.

Exhibit F Publications

MSI210379	Mann, C.C., "Homeland Insecurity," September 2002.
MSI210403	Boone, J.V.,et al., "The Start of Digital Revolution: SIGSALY Secure Digital Voice Communications in World War II," December 10, 2002.
MSI210421	Weadon, P.D., "The SIGSALY Story," December 10, 2002.
MSI210447	"iOpener," Registered Trademark of National Semiconductor Corporation, Registration date October 4, 1994.
MSI210496	Schill, A.B., et al., "DC++: Distributed Object-Oriented System Support on top of OSF DCE," 1993.
MSI210517	Schill, A.B., et al., "DCE-The OSF Distributed Computing Environment Client Server Model and Beyond," October 1993.
MSI210522	Rosenberry, W., et al., "Understanding DCE," 1992.
MSI210838	Karger, P.A., et al., "A VMM Security Kernel for the VAX Architecture," 1990.
MSI210856	Landwehr, C.E, et al., "A Taxonomy of Computer Program Security Flaws," September 1994.
MSI210900	Landwehr, C.E., "Formal Models for Computer Security," September 1981.
MSI210941	Young, W.D., "Verifiable Computer Security and Hardware: Issues," September 1991.
MSI210984	Cybenko, G, et al., "Cognitive Hacking: A Battle for the Mind," 2002.
MSI211023	National Security Agency, "Security Enhanced LINUX," December 10, 2002.
MSI211026	National Security Agency, "Korean War Commemoration," December 10, 2002.
MSI211071	National Security Agency, "Guide to the Secure Configuration and Administration of Microsoft Exchange 5.x®," June 20, 2002.
MSI211133	National Security Agency, "Microsoft Office 97 Executable Content Security Risks and Countermeasures," December 20, 1999.
MSI211180	Bartock, P.F., et al., "Guide to Securing Microsoft Windows NT Networks," September 18, 2001.
MSI211325	Bickel, R., et al., "Guide to Securing Microsoft Windows XP," October 30, 2002.

Exhibit F Publications

MSI211504	National Security Agency, "SIGSALY Secure Digital Voice Communications in World War II," December 10, 2002.
MSI211515	Distributed Computing Environment, "DCE Technology at Work," December 13, 2002.
MSI211582	Kent, S., "Part II: Certificate-Based Key Management," February 1993.
MSI213017	Saydjari, O.S., et al., "LOCK Trek: Navigating Unchartered Space," 1989.
MSI213026	Saydjari, O.S., et al., "LOCK Trek: Navigating Unchartered Space," 1989.
MSI213042	Karger, P.A., et al., "Multics Security Evaluation: Vulnerability Analysis," June 1974.
MSI213076	Aucsmith, D., et al., "Common Data Security Architecture," January 22, 1996.
MSI213088	Jaeger, T, et al., "Support for the File System Security Requirements of Computational E-Mail Systems," November 1994.
MSI213206	Tirkel, A.Z. et al., "Electronic Water Mark," (undated).
MSI213211	van Schyndel, R.G., et al., "A Digital Watermark," (undated).
MSI213214	Kurak, C., et al., "A Cautionary Note On Image Downgrading," 1992.

Exhibit G

EXHIBIT G - Patents

MSI023624-44
MSI023734-69
MSI023803-9
MSI029229
MSI029230
MSI036205-19
MSI080838-58
MSI082687-99
MSI088149
MSI088161
MSI088513
MSI088524-49
MSI088550
MSI089473-81
MSI089482-514
MSI089539-47
MSI089548
MSI089604
MSI089686-93
MSI089700-05
MSI089706-15
MSI089776
MSI089806-13
MSI089814-28
MSI089842-48
MSI089849-63
MSI089864-71
MSI160834-1126
MSI162608-29
MSI162630-45
MSI162959-3013
MSI163080-116
MSI163117
MSI163128-168
MSI163192-214
MSI163254-337
MSI163419
MSI163432
MSI163463
MSI163487

MSI163500
MSI163664
MSI163763
MSI163791
MSI168646
MSI168647-659
MSI168660-754
MSI173420-838
MSI184171-191
MSI187425-477
MSI187550-625
MSI2012502-22
MSI204898-932
MSI204933-965
MSI205493-499
MSI205500-522
MSI205828-844;
MSI212472-89
MSI205845-864
MSI207029-048
MSI207049-088
MSI210261-83
MSI210284-96
MSI210330-57
MSI210358-78
MSI210579-600
MSI210601-16
MSI210652-69
MSI211661-951
MSI212012-19
MSI212020-51
MSI212201-36
MSI212237-45
MSI212246-53
MSI212254-300
MSI212344-53
MSI212354-61
MSI212362-74
MSI212375-79
MSI212380-417

MSI212418-22
MSI212423-32
MSI212433-48
MSI212449-63
MSI212464-471
MSI2124690-501
MSI212615-41
MSI212642-62
MSI212663-74
MSI212675-97
MSI212698-706
MSI212736-43
MSI212744-61
MSI212762-69
MSI212770-78
MSI212779-90
MSI212791-807
MSI212808-40
MSI212841-60
MSI212861-76
MSI212877-87
MSI212888-901
MSI212902-10
MSI212911-21
MSI212922-49
MSI212950-62
MSI212963-73
MSI212974-3016
MSI213066-75
MSI213097-107
MSI213108-40
MSI213141-78
MSI213179-91
MSI213192-205
MSI213221-29
MSI213230-39
MSI213240-48
MSI213249-57
MSI213258-61

EXHIBIT G – MICROSOFT'S CORPORATION'S
PATENT LOCAL RULE 4-2 DISCLOSURE
(LIMITED TO "MINI-MARKMAN" CLAIMS),
CASE NO. C 01-1640 SBA

Exhibit G - Microsoft's Patent Local Rule 4-2 Disclosure (Limited to "Mini-Markman" Claims)

BATES NO.	PATENT NO.	ISSUE DATE	INVENTOR
MSI023624	5,138,712	August 11, 1992	Corbin
MSI023734	5,113,518	May 12, 1992	Durst, Jr. et al.
MSI023803	4,941,175	July 10, 1990	Enescu et al.
MSI029229	5,940,504	August 17, 1999	Griswold
MSI029230	4,020,326	April 26, 1977	Coulthurst
MSI036205	4,937,863	June 26, 1990	Robert et al.
MSI080838	4,827,508	May 2, 1989	Shear
MSI082687	4,609,777	September 2, 1986	Cargile
MSI088149	5,966,440	October 12, 1999	Hair
MSI088161	5,191,573	March 2, 1993	Hair
MSI088513	4,866,769	September 12, 1989	Karp
MSI088524	5,291,598	March 1, 1994	Grundy
MSI088550	5,014,234	May 7, 1991	Edwards, Jr.
MSI089473	3,996,449	December 7, 1976	Attanasio et al.
MSI089482	4,104,721	August 1, 1978	Markstein et al.
MSI089539	4,183,085	January 8, 1980	Roberts et al.
MSI089548	4,246,638	January 20, 1981	Thomas
MSI089604	4,442,484	April 10, 1984	Childs, Jr et al.
MSI089686	4,471,216	September 11, 1984	Herve
MSI089700	4,523,271	June 11, 1985	Levien
MSI089706	4,525,599	June 25, 1985	Curran et al.
MSI089776	4,562,305	December 31, 1985	Gaffney, Jr.
MSI089806	4,598,288	July 1, 1986	Yarbrough et al.
MSI089814	4,599,489	July 8, 1986	Cargile
MSI089842	4,609,985	September 2, 1986	Dozier
MSI089849	4,621,321	November 4, 1986	Boebert et al.
MSI089864	4,621,334	November 4, 1986	Garcia
MSI160834	5,603,031	February 11, 1997	White et al.
MSI162608	5,577,209	November 19, 1996	Boyle et al.
MSI162630	5,369,702	November 29, 1994	Shanton
MSI162959	5,206,951	April 27, 1993	Khoyi et al.
MSI163080	5,724,425	March 3, 1998	Chang et al.
MSI163117	4,995,082	February 19, 1991	Schnorr
MSI163128	5,689,565	November 18, 1997	Spies et al.
MSI163192	5,689,566	November 18, 1997	Nguyen
MSI163254	5,649,099	July 15, 1997	Theimer et al.
MSI163419	4,816,655	March 28, 1989	Musyck et al.
MSI163432	5,892,899	April 6, 1999	Aucsmith et al.
MSI163463	5,390,297	February 14, 1995	Barber et al.
MSI163487	5,956,408	September 21, 1999	Arnold
MSI163500	5,625,693	April 29, 1997	Rohatgi et al.
MSI163664	4,259,720	March 31, 1981	Campbell
MSI163763	4,321,672	March 23, 1982	Braun et al.
MSI163791	5,636,276	June 3, 1997	Brugger
MSI168646	5,956,408	September 21, 1999	Arnold (File History)
MSI168647	5,956,408	September 21, 1999	Arnold
MSI168660	5,956,408	September 21, 1999	Arnold (Application)
MSI173420	5,390,297	February 14, 1995	Barber et al.
MSI184171	5,365,587	November 15, 1994	Campbell et al.
MSI187425	5,373,440	December 13, 1994	Cohen et al.
MSI187550	5,557,798	September 17, 1996	Skeen et al.

Exhibit G - Microsoft's Patent Local Rule 4-2 Disclosure (Limited to "Mini-Markman" Claims)

MSI212502	5,490,216	February 6, 1996 Richardson, III
MSI204898	5,715,314	February 3, 1998 Payne et al.
MSI204933	5,724,424	March 3, 1998 Gifford
MSI205493	5,432,851	July 11, 1995 Scheidt et al.
MSI205500	5,369,707	November 29, 1994 Follendore, III
MSI205828	5,432,928	July 11, 1995 Sherman
MSI212472	5,432,928	July 11, 1995 Sherman
MSI205845	5,301,326	April 5, 1994 Linnett et al.
MSI207029	5,319,735	June 7, 1994 Preuss et al.
MSI207049	5,450,490	September 12, 1995 Jensen et al.
MSI210261	5,164,988	November 17, 1992 Matyas et al.
MSI210284	5,699,427	December 16, 1997 Chow et al.
MSI210330	4,926,480	May 15, 1990 Chaum
MSI210358	4,529,870	July 16, 1985 Chaum
MSI210579	5,361,359	November 1, 1994 Tajalli et al.
MSI210601	5,325,524	June 28, 1994 Black et al.
MSI210652	5,802,590	September 1, 1998 Draves
MSI211661	6,016,393	January 18, 2000 White et al.
MSI212012	5,199,074	March 30, 1993 Thor
MSI212020	5,367,621	November 22, 1994 Cohen et al.
MSI212201	5,129,084	July 7, 1992 Kelly, Jr. et al.
MSI212237	5,150,407	September 22, 1992 Chan
MSI212246	5,199,066	March 30, 1993 Logan
MSI212254	5,204,897	April 20, 1993 Wyman
MSI212344	5,263,157	November 16, 1993 Janis
MSI212254	5,263,165	November 16, 1993 Janis
MSI212362	5,276,901	January 4, 1994 Howell et al.
MSI212370	5,283,830	February 1, 1994 Hinsley et al.
MSI212375	5,287,407	February 15, 1994 Holmes
MSI212380	5,335,346	August 2, 1994 Fabbio
MSI212418	5,337,357	August 9, 1994 Chou et al.
MSI212423	5,343,526	August 30, 1994 Lassers
MSI212433	5,349,642	September 20, 1994 Kingdon
MSI212449	5,359,721	October 25, 1994 Kempf et al.
MSI212464	5,371,792	December 6, 1994 Asai et al.
MSI212490	5,440,634	August 8, 1995 Jones et al.
MSI212615	5,845,281	December 1, 1998 Benson et al.
MSI212642	4,529,870	July 16, 1985 Chaum
MSI212663	4,573,119	February 25, 1986 Westheimer et al.
MSI212675	4,578,530	March 25, 1986 Zeidler
MSI212698	4,590,552	May 20, 1986 Guttag et al.
MSI212736	4,683,968	August 4, 1987 Appelbaum et al.
MSI212744	4,780,821	October 25, 1988 Crossley
MSI212762	4,796,220	January 3, 1989 Wolfe
MSI212770	4,864,616	September 5, 1989 Pond et al.
MSI212779	4,868,736	September 19, 1989 Walker
MSI212791	4,888,798	December 19, 1989 Earnest
MSI212808	4,893,248	January 9, 1990 Pitts et al.
MSI212841	4,893,332	January 9, 1990 Brown
MSI212861	4,953,209	August 28, 1990 Ryder, Sr. et al.
MSI212877	4,962,533	October 9, 1990 Krueger et al.
MSI212888	4,975,878	December 4, 1990 Boddu et al.
MSI212902	5,022,080	June 4, 1991 Durst et al.
MSI212911	5,027,397	June 25, 1991 Double et al.

Exhibit G - Microsoft's Patent Local Rule 4-2 Disclosure (Limited to "Mini-Markman" Claims)

MSI212922	5,032,979	July 16, 1991	Hecht et al.
MSI212950	5,058,162	October 15, 1991	Santon et al.
MSI212963	5,065,429	November 12, 1991	Lang
MSI212974	5,109,413	April 28, 1992	Comerford et al.
MSI213066	5,383,113	January 17, 1995	Kight et al.
MSI213097	5,524,933	June 11, 1996	Kunt et al.
MSI213108	4,672,605	June 9, 1987	Hustig et al.
MSI213141	5,103,459	April 7, 1992	Gilhousen et al.
MSI213179	3,845,391	October 29, 1974	Crosby
MSI213192	DE 29 43 436 A1	October 26, 1979 (filed)	Szepanski
MSI213221	5,574,962	November 12, 1996	Fardeau et al.
MSI213230	5,581,800	December 3, 1996	Fardeau et al.
MSI213240	5,787,334	July 28, 1998	Fardeau et al.
MSI213249	5,721,788	February 24, 1998	Powell et al.
MSI213258	5,079,648	January 7, 1992	Maufe

1 KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
2 MICHAEL H. PAGE - #154913
710 Sansome Street
3 San Francisco, CA 94111-1704
Telephone: (415) 391-5400
4 Facsimile: (415) 397-7188

5 DERWIN & SIEGEL
DOUGLAS K. DERWIN - #111407
6 3280 Alpine Road
Portola Valley, CA 94028
7 Telephone: (650)529-8700
Facsimile: (650) 529-8799
8
INTERTRUST TECHNOLOGIES CORPORATION
9 MARK SCADINA - #173103
JEFF MCDOW - #184727
10 4800 Patrick Henry Drive
Santa Clara, CA 95054
11 Telephone: (408) 855-0100
Facsimile: (408) 855-0144
12
Attorneys for Plaintiff and Counter-Defendant
13 INTERTRUST TECHNOLOGIES CORPORATION

14

15   UNITED STATES DISTRICT COURT

16   NORTHERN DISTRICT OF CALIFORNIA

17

18 INTERTRUST TECHNOLOGIES   Case No. C 01-1640 SBA (MEJ)
    CORPORATION, a Delaware corporation,
19   Consolidated with C 02-0647 SBA
                            Plaintiff,
20   **PATENT LOCAL RULE 4-3 JOINT
        v.   CLAIM CONSTRUCTION AND
21   PREHEARING STATEMENT**

22 MICROSOFT CORPORATION, a
    Washington corporation,
23
                            Defendant.
24 _____

25 AND COUNTER ACTION.

26

27

28

1   Plaintiff and Counter-Defendant Intertrust Technologies Corporation ("Intertrust") and

2   Defendant and Counter-Claimant Microsoft Corporation ("Microsoft") submit the following

3   Joint Claim Construction and Prehearing Statement in accordance with Patent Local Rule 4-3.

RULE 4-3(a) and (b)

5   Claim terms and phrases on which the parties agree are listed at the beginning of Exhibit

6   B, attached.

RULE 4-3(b)

8   Attached hereto as Exhibit A is Microsoft's presentation of disputed claim terms

9   and Microsoft's proposed constructions. Attached hereto as Exhibit B is InterTrust's

10   presentation of disputed claim terms and InterTrust's proposed constructions. The parties are

11   discussing a joint presentation that would present each party's position on all disputed terms in a

12   side-by-side format. If the parties reach agreement on such a submission, the parties will provide

13   that submission to the Court as a substitute for the attached Exhibits A and B.

14   Attached hereto as Exhibit C is InterTrust's identification of intrinsic and

15   extrinsic evidence supporting InterTrust's proposed construction for each disputed term and

16   phrase.

17   Attached hereto as Exhibit D is Microsoft's identification of intrinsic and

18   extrinsic evidence supporting Microsoft's proposed construction for each disputed term and

19   phrase.

20   Attached hereto as Exhibit E is a Microsoft statement of reservations.

RULE 4-3(c)

22   The Court has set aside three days for the Claim Construction Hearing.

RULE 4-3(d)

24   Attached hereto as Exhibit F is a summary of expert testimony to be presented by

25   InterTrust. Attached hereto as Exhibit G·is a summary of expert testimony to be presented by

26   Microsoft.

RULE 4-3(e)

28   Following is a list of other issues the parties believe might appropriately be taken

1

up at the Case Management Conference hearing set for February 13, or such other prehearing conference as the Court may wish to schedule. Substantive argument on these issues is set forth in the Joint Case Management Conference Statement filed concurrently herewith.

A. Issues upon which the parties agree:

1. Live expert testimony should not be presented. Each party will undertake its best efforts to have its above-designated expert(s) present at the hearing to respond to questions from the Court.

2. Each party will undertake its best efforts to have its declarants available for deposition within one week of submitting Claim Construction or indefiniteness summary judgment declarations.

3. Normal briefing page limits should be doubled for the Claim Construction briefs.

4. There will be no post-hearing briefing, except at the request of the Court.

B. Issues which the parties agree should be taken up at the Case Management Conference, but as to which the parties do not agree on substance:

1. The number of claim construction briefs to be filed by the parties.

2. Format of the Claim Construction Hearing.

a. Whether the parties should present tutorials, and, if so, the length and format of such a tutorial.

b. Whether the parties should present a non-tutorial opening statement.

c. The format and ordering of substantive argument on disputed claim language.

d. Whether the currently scheduled Mini-Markman proceeding should be devoted to all of the disputed terms and phrases from the 12 selected patent claims, or a subset.

3. Whether other issues should be addressed during the Claim Construction Hearing.

    a. The anticipated Microsoft motion for summary judgment of indefiniteness, referenced in the Court's Further Case Management Order of November 6, 2002.

    b. Whether certain material said to be "incorporated by reference" into several of the asserted patents, does or does not constitute part of the "specification" of those patents for claim construction purposes.

    c. Other evidentiary disputes related to the Claim Construction Hearing.

C. Issues Microsoft intends to raise at the Case Management Conference, but which InterTrust believes are not appropriate for that conference:

    1. Claim construction and claim indefiniteness discovery disputes.

    2. The scope of the stay entered by the court.

Respectfully submitted,

Dated: February 3, 2003   KEKER & VAN NEST, LLP

By: _____
MICHAEL H. PAGE
Attorneys for Intertrust Technologies
Corporation

Dated: February 3, 2003   ORRICK HERRINGTON & SUTCLIFFE

By: _____ *BY PHONE AUTHORITY*
ERIC L. WESENBERG
Attorneys for Microsoft Corporation

305966.01

Exhibit A

Exhibit A contains Microsoft's Preliminary Claim Construction. The chart presents the construction in the order of the asserted "Mini-Markman" claims. Terms set forth in the claims (column 2) in bold are claim terms that the parties dispute. Phrases set forth in the claims in italics are claim phrases that the parties dispute. Terms set forth in Microsoft's construction (column 3) in bold, with initial capitalizaiton are terms Microsoft has construed.

'193 Asserted Claim 1

	'193 Claim 1	**MS Construction**
1.	1. A method comprising:	Claim as a whole: The recited method is performed within a VDE. (See item #93 for Microsoft's construction of VDE.)
2.	*receiving a digital file including music,*	receiving a digital file including music: This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites a step or result ("receiving") without reciting an action that achieves that result. The specification does not clearly link any particular action to this recited step. Part of the recited function is performed when the Digital File is received by Communications Controller 666 and passed through I/O Controller 600 to SPE 503/SPU 500 (specifically incorporates the SPU Encryption/Decryption Engine 522 that is used principally as an aspect of secure communications between VDE secure subsystems) and NVRAM 534b (which stores sensitive information such as cryptographic Key(s) used for Authentication.) Rights Operating System 602 manages the hardware within SPU 500 that performs Authentication of the secure container as part of the receiving step. The recited function requires: obtaining a VDE Secure Container encapsulating a Digital File, Authenticating the intended recipient in accordance with VDE Controls Associated With the Secure Container, and accepting the Secure Container. The qualifier "including music" recites non-functional descriptive material and is not a patentable limitation. digital file: A named, static unit of storage allocated by a "file system" and Containing digital information. A Digital File enables any application using the "file system" to randomly access its contents and to distinguish it by name from every other such unit. A copy of a Digital File is a separate Digital File. (A "file system" is the portion of the operating system that translates requests made by application programs for operations on "files" into low-level tasks that can control storage devices such as disk drives.) including: As to data, storing within, as opposed to Addressing. As to hardware, physically present within.
3.	storing said **digital file** in a first **secure memory** of a first device;	digital file: see item #2 above secure memory: A processor-addressable Memory within a special-purpose Secure Processing Unit which is isolated from the rest of the world by (and encapsulated within) a Tamper Resistant Barrier. "Processor-addressable" means that a connected processor can use the Secure Memory's physical addresses as the operand in a processor instruction such as LOAD or STORE or equivalent instruction. A "Memory" is not a "Secure Memory" merely because it stores encrypted, signed, and/or sealed data; is accessible from a Protected Processing Environment; or is within an appliance that is located at a trusted facility with non-VDE physical Security and user-identity Authentication procedures.

		'193 Claim 1	MS Construction
			secure: A state in which all users of a system are guaranteed that all information, processes, and devices within the system, shall have their availability, secrecy, integrity, authenticity and nonrepudiation maintained against all of the identified threats thereto. "Availability" means the property that information is accessible and usable upon demand by authorized persons, at least to the extent that no user may delete the information without Authorization. "Secrecy," also referred to as confidentiality, means the property that information (including computer processes) is not made available or disclosed to unauthorized persons or processes. "Integrity" means the property that information has not been altered either intentionally or accidentally. "Authenticity" means the property that the characteristics asserted about a person, device, program, information, or process are genuine and timely, particularly as to identity, data integrity, and origin integrity. "Nonrepudiation" means the property that a sender of information cannot deny its origination and that a recipient of information cannot deny its receipt. memory: A medium in which data (including executable instructions) may be stored and from which it may be retrieved.
4.		storing information associated with said digital file in a secure database stored on said first device,	associated with: A specific, direct, persistent, and binding relationship with one or more discrete items. Code that processes information but is merely a general-purpose component of an installation is not "Associated With" that information. In VDE, an association between a unit of Executable code and particular information, or between particular control information and a Secure Container, cannot be broken except as Allowed by execution (within a Secure Processing Environment) of assigned VDE Control(s) and satisfaction of all requirements imposed by such execution. digital file: see item #2 above secure database: A Secure Database is a database isolated from all users such that it is Protected from external observation; and accidental or intentional alteration or destruction. In VDE, a Secure Database stores tracking, billing, payment, and auditing data until the data is delivered Securely to an authorized Clearinghouse. secure: see item #3 above database: a data file that is defined and accessed using the facilities of a database management system (DBMS); this implies in particular (a) that it is defined by means of a schema that is independent of any programs that access the database, and (b) that it uses direct access storage.
5.		said information including at least one budget control and at least one copy control,	including: see item #2 above budget: A unique type of "method" that specifies a decrementable numerical limitation on future Use (e.g., copying) of digital information and how such Use will be paid for, if at all. (A "method" is a collection of basic instructions, and information related to basic instructions, that provides context, data, requirements, and/or relationships for use in performing, and/or preparing to perform, basic instructions in relation to the operation of one or more electronic appliances.) budget control: A VDE Control assembled to apply to a Budget, and enforcing that Budget. No process, user, or device is able to make the use identified by the Budget once the Budget's specified limitation on that Use has been reached. copy control: A VDE Control which Controls Access to or some Use of a copy.
6.		said at least one budget control including *a budget specifying the number of*	a budget specifying the number of copies which can be made of said digital file: A Budget explicitly stating the total number of copies (whether or not decrypted, long-lived, or accessible) that (since creation of the Budget) Can Be made of the Digital

	'193 Claim 1	MS Construction
	copies which can be made of said digital file;	File by any and all users, devices, and processes. No process, user, or device is able to make another copy of the Digital File once this number of copies has been made. budget, budget control: see item #5 above including: see item #2 above can be: A specified act is able or authorized to be carried out, which otherwise cannot be carried out. digital file: see item #2 above
7.	and said at least one copy control *controlling the copies made of said digital file;*	controlling the copies made of said digital file: Controlling Uses of and Accesses to all copies of the Digital File, by all users, processes, and devices, by executing each of the recited "at least one" Copy Control(s) within VDE Secure Processing Environment(s). Each Control Governs (Controls) only one action, which action may or may not differ among the different "at least one" Controls. All Uses and Accesses are prohibited and incapable of occurring except to the extent Allowed by the "at least one" Copy Control(s). copy control: see item #5 above controlling: Reliably defining and enforcing the conditions and requirements under which an action that otherwise cannot be taken, will be Allowed, and the manner in which it may occur. Absent verified satisfaction of those conditions and requirements, the action cannot be taken by any user, process or device. In VDE, an action is Controlled through execution of the applicable VDE Control(s) within a VDE Secure Processing Environment. More specifically, in VDE, Controlling is effected by use of VDE Controls, VDE Secure Containers, and VDE foundation (including VDE Secure Processing Environment, "object registration," and other mechanisms for allegedly individually ensuring that specific Controls are enforced vis-à-vis specific objects (and their content at an arbitrary granular level) and specific "users.") digital file: see item #2 above
8.	*determining whether said digital file may be copied and stored on a second device based on at least said copy control;*	determining whether said digital file may be copied and stored on a second device based on at least said copy control: Determining whether this particular first device is Allowed to perform both of the following actions on this particular Digital File: (1) Copy it and (2) store it (as opposed to a copy of it) on a second device, by executing one or more VDE Control(s) (including "said" Copy Control Associated With this Digital File) within VDE Secure Processing Environment(s). To the extent that either of these two actions is not determined by this step to be permissible, that action is prohibited and incapable of occurring, and no user, process or device can perform it on this Digital File. This claim limitation's recitation of "said copy control" is inconsistent with the claim limitation "at least one copy control." digital file: see item #2 above copy, copied, copying: To reproduce all of a Digital File or other complete physical block of data from one location on a storage medium to another location on the same or different storage medium, leaving the original block of data unchanged, such that two distinct and independent objects exist. Although the layout of the data values in physical storage may differ from the original, the resulting "copy" is logically indistinguishable from the original. The resulting "copy" may or may not be encrypted, ephemeral, usable, or accessible.

	'193 Claim 1	MS Construction
		copy control: see item #5 above
9.	*if said copy control allows at least a portion of said digital file to be copied and stored on a second device,*	if said copy control allows at least a portion of said digital file to be copied and stored on a second device: This "if" condition creates two branches for the recited process, each of which must be performed. Each time the "if" condition is met, all four of the later-recited actions (Copying, transferring, storing, playing) must occur. Each time it is not met, each of these four actions must be prohibited and incapable of occurring. This "if" condition is met if and only if "said" Copy Control Allows any Portion (i.e., a part less than the whole) of the Digital File to be Copied and also Allows that same Portion of the Digital File (as opposed to the copy) to be stored on any second device. This "if" condition is based entirely on "said copy control" and thus is met, as above, even if other VDE Control(s) prohibit those actions. This claim limitation's recitation of "copy control allows at least a portion" is inconsistent with the claim limitation "whether said digital file may be copied ... based on at least said copy control." This claim limitation's recitation of "if said copy control allows at least a portion ... copying" is inconsistent with "said at least one budget control including a budget specifying the number of copies which can be made of said digital file" on whether said "copy control" or said "budget control" determines whether Copying is Allowed. copy control: see item #5 above allow (allows): Actively permitting an action that otherwise cannot be taken (i.e., is prohibited) by any user, process, or device. In VDE, an action is Allowed only through execution (within a Secure Processing Environment) of the VDE Control(s) assigned to the particular action request, and satisfaction of all requirements imposed by such execution. portion: A part of a whole, which is less than the whole digital file: see item #2 above
10.	*copying at least a portion of said digital file;*	copying at least a portion of said digital file: Copying at least some Portion of the Digital File (as opposed to a copy thereof), by executing VDE Control(s) within VDE Secure Processing Environment(s). This Copied "Portion" may or may not be (or even include) the Portion referred to in the claim limitation "if said copy control allows at least a portion." copying: see item #8 above portion: see item #9 above digital file: see item #2 above
11.	*transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;*	transferring at least a portion of said digital file to a second device: Transferring to some second device (which may or may not be the "second device" referred to in the claim limitation "if said copy control allows at least a portion of said digital file to be copied and stored on a second device") at least some Portion of the Digital File (as opposed to a copy thereof), by executing VDE Control(s) within VDE Secure Processing Environment(s). This transferred Portion may or may not be (or even include) the Portion referred to in the claim limitation "if said copy control allows at least a portion," or the Portion referred to in the claim limitation "copying at least a portion."

EXHIBIT A TO JOINT CLAIM CONSTRUCTION STATEMENT

	'193 Claim 1	MS Construction
		portion: see item #9 above
		digital file: see item #2 above
		memory: see item #3 above
12.	*storing said digital file* in said **memory** of said second device; and	storing said digital file: Storing the entire Digital File received in the "receiving" step (as opposed to a copy of the Digital File or a Portion of the Digital File). This claim limitation's recitation of "storing said digital file" is inconsistent with the claim limitation "transferring at least a portion of said digital file."
		digital file: see item #2 above
		memory: see item #3 above
13.	including playing said music through said audio output	This claim limitation's recitation of "playing ... through said audio output" is inconsistent with the claim limitation "an audio and/or video output."

	'193 - Claim 11	MS Construction
14.	11. A method comprising:	Claim as a whole: The recited method is performed within a VDE. (See item #93 for Microsoft's construction of VDE.)
15.	*receiving a digital file*	receiving a digital file: see item #2 above digital file: see item #2 above
16.	storing information associated with said digital file in a secure database stored on said first device,	associated with: see item #4 above digital file: see item #2 above secure database: see item #4 above
17.	said information including a first control;	including: see item #2 above control: Independent, special-purpose, Executable, which can execute only within a Secure Processing Environment. Each VDE Control is a Component Assembly dedicated to a particular activity (e.g., editing, modifying another Control, a user-defined action, etc.), particular user(s), and particular Protected information, and whose satisfactory execution is necessary to Allowing that activity. Each separate information Access or Use is independently Controlled by independent VDE Control(s). Each VDE Control is assembled within a Secure Processing Environment from independently deliverable modular components (e.g., Load Modules or other Controls), dynamically in response to an information Access or Use Request. The dynamic assembly of a Control is directed by a "blueprint" Record (put in place by one or more VDE users) Containing control information identifying the exact modular code components to be assembled and executed to Govern this particular activity on this particular information by this particular user(s). Each Control is independently assembled, loaded and delivered vis-à-vis other Controls. Control information and Controls are extensible and can be configured and modified by all users, and combined by all users with any other VDE Control information or Controls (including that provided by other users), subject only to "senior" user Controls. Users can assign control information (including alternative control information) and controls to an arbitrarily fine, user-defined Portion of the Protected information, such as a single paragraph of a document, as opposed to being limited to file-based Controls. VDE Controls reliably limit Use of the Protected information to Authorized activities and amounts.
18.	*determining whether said digital file may be copied and stored on a second device based on said first control,*	determining whether said digital file may be copied and stored on a second device based on said first control: Determining whether said first Control, by itself, Allows this particular first device to perform both of the following actions on this particular Digital File: (1) Copy it and (2) store it (as opposed to a copy of it) on a second device, by executing the first VDE Control within VDE Secure Processing Environment(s). To the extent that either the Copy or store action is not determined by this step to be permissible, that action is prohibited and incapable of occurring, and no user, process or device can perform it on this Digital File. digital file: see item #2 above copied: see item #10 above control: see item #17 above
19.	said determining step including *identifying said second device* and	identifying said second device: Identifying a second device sufficiently to distinguish it from all other devices, by executing VDE Control(s) within VDE Secure Processing Environment(s).

EXHIBIT A TO JOINT CLAIM CONSTRUCTION STATEMENT
Page 6 of 37

	'193 - Claim 11	MS Construction
	determining *whether said first control allows transfer of said copied file to said second device,*	whether said first control allows transfer of said copied file to said second device Whether the first Control, by itself, Allows the entire Digital File (which has been Copied at least once) (as opposed to the copy) to be moved to the identified second device. If not, that transfer is prohibited and incapable of occurring and no user, process or device can perform that action on this Digital File. Identifying/identify: To establish as being a particular instance of a person or thing control: see item #17 above allow: see item #9 above copied file: A Digital File that has been Copied. The "copied file" is not the copy itself. A "copy" is what is formed by a Copying operation, and it may or may not be encrypted, ephemeral, usable, or accessible.
20.	*said determination based at least in part on the features present at the device to which said copied file is to be transferred;*	said determination based at least in part on the features present at the device: Basing the determination at least in part upon all actual, current features of the device (as opposed to previously determined, reported, or measured features) which might affect the device's ability to prevent Unauthorized Access to or Use of (or both) the Digital File. This determination is done without trusting either the device or any user of the device. A device Identifier such as a serial number is not a "feature present at the device." copied file: see item #19 above
21.	*if said first control allows at least a portion of said digital file to be copied and stored on a second device,*	if said first control allows at least a portion of said digital file to be copied and stored on a second device: This "if" condition creates two branches for the recited process, each of which must be performed. Each time the "if" condition is met, all four of the later-recited actions (Copying, transferring, storing, Rendering) must occur. Each time it is not met, each of these four actions must be disabled and prohibited and incapable of occurring. This "if" condition is met if and only if the first Control allows any Portion of the Digital File to be Copied and also allows that same Portion of the Digital File (as opposed to the copy) to be on any second device. This "if" condition is based entirely on the first Control and thus is met, as above, even if other VDE Controls prohibit those actions. This claim limitation's recitation of "said first control allows at least a portion" is inconsistent with the claim limitation "whether said digital file may be copied ... based on said first control." control: see item #17 above allow: see item #9 above portion: see item #9 above digital file: see item #2 above
22.	*copying at least a portion of said digital file;*	copying at least a portion of said digital file: see item #10 above copying: see item #8 above portion: see item #9 above

	'193 - Claim 11	MS Construction
		digital file: see item #2 above
23.	*transferring at least a portion of said digital file to a second device* including a memory and an audio and/or video output;	transferring at least a portion of said digital file to a second device: see item #11 above portion: see item #9 above digital file: see item #2 above memory: see item #3 above
24.	*storing said digital file in* said memory of said second device; and	storing said digital file: see item #12 above digital file: see item #2 above
25.	rendering said digital file through said output.	rendering: Playing content through an audio output (e.g., speakers) or displaying content on a video output (e.g., a screen). digital file: see item #2 above This claim limitation's recitation of "said output" is inconsistent with the claim limitation "an audio and/or video output."

	'193 Claim 15	MS Construction
26.	15. A method comprising:	**Claim as a whole:** The recited method is performed within a VDE. (See item #93 for Microsoft's construction of VDE.)
27.	*receiving a digital file;*	receiving a digital file: see item #2 above This step must proceed in both "Authentication branches" of the process (i.e., regardless of the outcome of the "Authentication" step). digital file: see item #2 above
28.	*an authentication step comprising:*	an authentication step comprising: Authenticating the first device and/or user of the first device without relying on trusting either, by executing VDE Control(s) within VDE Secure Processing Environment(s). authentication: To establish that the following asserted characteristics of something (e.g., a person, device, organization, document, file, etc.) are genuine: its Identity, its data integrity, (i.e., it has not been altered) and its origin integrity (i.e., its source and time of origination).
29.	*accessing at least one identifier associated with a first device or with a user of said first device; and*	accessing at least one identifier associated with a first device or with a user of said first device: Securely Accessing at least one Identifier Associated With a single ("first") device or (as opposed to "and") with a single, current user of that device, by executing VDE Control(s) within VDE Secure Processing Environment(s). One of the "at least one identifier" may be Associated With a first device while another of the "at least one identifier" may be Associated With a user of said first device. Access (accessing): To satisfactorily perform the steps necessary to obtain something so that it can be Used in some manner (e.g., for information: copied, printed, decrypted, encrypted, saved, modified, observed, or moved, etc.). In VDE, access to protected information is achieved only through execution (within a Secure Processing Environment) of the VDE Control(s) assigned to the particular "access" request, satisfaction of all requirements imposed by such execution, and the Controlled Opening of the Secure Container Containing the information. identifier: Any text string used as a label naming an individual instance of what it Identifies. associated with: see item #4 above
30.	*determining whether said identifier is associated with a device and/or user authorized to store said digital file;*	determining whether said identifier is associated with a device and/or user authorized to store said digital file: For each accessed "at least one identifier," determining whether the device with which it is Associated is one on which the Digital File may be stored (by any user) and/or whether the user with which it is Associated is one who may store the Digital File (on any device), by executing VDE Control(s) within VDE Secure Processing Environment(s). Each Identifier may be Associated With a device "and" a user, or with a device only, or with a user only. This claim limitation's recitation of "said identifier" is inconsistent with the claim limitation "at least one identifier." identifier: see item #29 above associated with: see item #4 above authorized: An action is permitted that otherwise cannot be taken by any user, process, or device. In VDE, an action is authorized only through execution of the applicable VDE Control(s) within a VDE Secure Processing Environment and

	'193 Claim 15	MS Construction
		satisfaction of all requirements imposed by such execution.
		"not authorized": The action is prohibited and cannot be taken by any user, process, or device.
		<u>digital file</u>: see item #2 above
31.	*storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized;*	<u>storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized</u>: This conditional step creates at least two "Authentication" branches for the recited process, each of which must be performed. Each time the condition is met, the recited "storing" must occur. Each time it is not met, the recited "storing" must not occur.
		If "storing" proceeds, then: storing in a **Secure Memory** of the first device, the entire **Digital File** received in the "receiving" step, as opposed to a copy of the File or a Portion of the Digital File, by executing **VDE Control(s)** within **VDE Secure Processing Environment(s)**. If "storing" does not proceed: then the Digital File is not stored in the **Secure Memory** of the first device, and is prevented from being stored anywhere on the first device.
		This limitation is internally inconsistent on the circumstances under which the storing proceeds or does not proceed. For example, the first ("only if") phrase requires that the storing step proceeds if the device is **Authorized** (and the user is not) while the second ("but not") phrase requires that the storing step not proceed if the device is **Authorized** (and the user is not).
		<u>authorized</u>: see item #30 above
		<u>digital file</u>: see item #2 above
		<u>secure memory</u>: see item #3 above
32.	*storing information associated with said digital file in a secure database stored on said first device, said information including at least one control;*	<u>storing information associated with said digital file in a secure database stored on said first device, said information including at least one control</u>: Storing information in a **Secure Database**, the entirety of information (including the "at least one Control") being **Associated With** the Digital File (as opposed to the file's contents independent of the file), by executing **VDE Control(s)** within **VDE Secure Processing Environment(s)**.
		This step must proceed in both "Authentication branches" of the process (i.e., regardless of the outcome of the "Authentication" step).
		<u>associated with</u>: see item #4 above
		<u>digital file</u>: see item #2 above
		<u>secure database</u>: see item #4 above
		<u>control</u>: see item #17 above
33.	*determining whether said digital file may be copied and stored on a second device based on said at least one control;*	<u>determining whether said digital file may be copied and stored on a second device based on said at least one control</u>: see item #8 above
		This step must proceed in both "Authentication branches" of the process (i.e., regardless of the outcome of the "Authentication" step).
		<u>digital file</u>: see item #2 above

	'193 Claim 15	MS Construction
		copied: see item #10 above
		control: see item #17 above
34.	*if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,*	if said at least one control allows at least a portion of said digital file to be copied and stored on a second device: see item #9 above
		control: see item #17 above
		allow: see item #9 above
		portion: see item #9 above
		digital file: see item #2 above
		copied: see item #10 above
35.	*copying at least a portion of said digital file;*	copying at least a portion of said digital file: see item #10 above
		copying: see item #8 above
		portion: see item #9 above
		digital file: see item #2 above
36.	*transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;*	transferring at least a portion of said digital file to a second device: see item #11 above
		This step must proceed in both "Authentication branches" of the process (i.e., regardless of the outcome of the "Authentication" step).
		portion: see item #9 above
		digital file: see item #2 above
		memory: see item #3 above
37.	*storing said digital file in said memory of said second device; and*	storing said digital file: see item #12 above This step must proceed in both "Authentication branches" of the process (i.e., regardless of the outcome of the "Authentication" step). This claim limitation's recitation of "storing said digital file" is inconsistent with the claim limitation "transferring at least a portion of said digital file."
		digital file: see item #2 above
		memory: see item #3 above
38.	*rendering said digital file through said output.*	rendering: see item #25 above
		digital file: see item #2 above
		This claim limitation's recitation of "said output" is inconsistent with the claim limitation "an audio and/or video output."

	'193 Claim 19	MS Construction
39.	19. A method comprising:	**Claim as a whole:** The recited method is performed within a VDE. (See item #93 for Microsoft's construction of VDE.)
40.	*receiving a digital file at a first device;*	**receiving a digital file at a first device:** see item #2 above **digital file:** see item #2 above
41.	*establishing communication between said first device and a clearinghouse located at a location remote from said first device;*	**establishing communication between said first device and a clearinghouse located at a location remote from said first device:** This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites a step or result ("establishing communication") without reciting an action that achieves that result. The specification does not clearly link any particular action to this recited step. Part of the recited function is performed by the Remote Procedure Call Manager 732 software of Rights Operating System 602 that controls I/O controller 660 and Communications Controller 666. Remote Procedure Call Manager handles all communication between VDE processes. The recited function is: creating and using a previously non-existent communications channel which is necessary and sufficient for exchanging information between the first device and a Clearinghouse. **clearinghouse:** A computer system that provides intermediate storing and forwarding services for both content and audit information, and which two or more parties trust to provide its services independently because it is operated under constraint of VDE Security. "Audit information" means all information created, stored, or reported in connection with an "auditing" process. "Auditing" means tracking, metering and reporting the usage of particular information or a particular appliance.
42.	said first device obtaining **authorization information** including a key from said clearinghouse;	**authorization information:** "Control information" identifying the exact modular code components to be assembled into a VDE Control and executed within a Secure Processing Environment to permit a particular activity that otherwise cannot be taken (i.e., is prohibited). ("Control information" is information which Identifies the exact modular code components and data which must be assembled and executed to Control a particular activity on particular information, of arbitrary, user-defined granularity, by particular user(s)). **key:** A bit sequence used and needed by a cryptographic algorithm to encrypt a block of plain text or to decrypt a block of cipher text. A Key is different from a key seed or other information from which the actual encryption and/or decryption Key is constructed, derived, or otherwise identified. In symmetric key cryptography, the same key is used for both encryption and decryption. In asymmetric or "public key" cryptography, two related keys are used; a block of text encrypted by one of the two keys (e.g., the "public key") can be decrypted only by the corresponding key (e.g., the "private key"). **clearinghouse:** see item #41 above
43.	said first device *using said authorization information to gain access to or make at least one use of said first digital file,*	**using said authorization information to gain access to or make at least one use of said first digital file:** A user, process or device uses all of said Authorization Information in connection with executing VDE Control(s) within VDE Secure Processing Environment(s) to gain Access to or (as opposed to "and") make at least one Use of the Digital File received in the "receiving" step. Without using such Authorization Information, no Access to or Use of the file is Allowed. **authorization information:** see item #42 above **access:** see item #29 above

	'193 Claim 19	MS Construction
		use: To use information is to perform some action on it or with it (e.g., copying, printing, decrypting, encrypting, saving, modifying, observing, or moving, etc.). In VDE, information Use is Allowed only through execution of the applicable VDE Control(s) and satisfaction of all requirements imposed by such execution. **digital file:** see item #2 above
44.	*including using said key to decrypt at least a portion of said first digital file;* and	**including using said key to decrypt at least a portion of said first digital file:** The "at least one use of said digital file" must encompass decrypting at least a Portion of the Digital File using the Key. **portion:** see item #9 above **digital file:** see item #2 above
45.	*receiving a first control from said clearinghouse at said first device;*	**receiving a first control from said clearinghouse at said first device:** This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites a step or result ("receiving") without reciting an action that achieves that result. The specification does not clearly link any particular action to this recited step. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b). The recited function requires: obtaining a VDE Secure Container encapsulating a first Control, authenticating the first device in accordance with VDE Controls Associated With the Secure Container, and accepting the Secure Container. **control:** see item #17 above **clearinghouse:** see item #41 above
46.	*storing said first digital file in a memory of said first device;*	**storing said first digital file in a memory of said first device:** Storing in a Memory of the first device, the entire Digital File (as opposed to a Portion thereof) received in the "receiving" step, by executing VDE Control(s) within VDE Secure Processing Environment(s). **digital file:** see item #2 above **memory:** see item #3 above
47.	*using said first control to determine whether said first digital file may be copied and stored on a second device;*	**using said first control to determine whether said first digital file may be copied and stored on a second device:** Determining whether the first Control, by itself, allows this particular first device to perform both of the following actions on this particular Digital File: (1) Copy it and (2) store it (as opposed to a copy of it) on a second device, by executing the first VDE Control within VDE Secure Processing Environment(s). To the extent that either the Copy or store action is not determined by this step to be permissible, that action is prohibited and incapable of occurring, and no user, process or device can perform it on this Digital File. **control:** see item #17 above **digital file:** see item #2 above **copied:** see item #10 above
48.	*if said first control allows at least a portion of said*	**if said first control allows at least a portion of said first digital file to be copied and stored on a second device:** see item #9 above

	'193 Claim 19	MS Construction
	first digital file to be copied and stored on a second device,	This claim limitation's recitation of "first control allows at least a portion of said first digital file" is inconsistent with the claim limitation "whether said first digital file may be copied ... on a second device." control: see item #17 above allow: see item #9 above portion: see item #9 above digital file: see item #2 above copied : see item #10 above
49.	*copying at least a portion of said first digital file;*	copying at least a portion of said first digital file: see item #10 above copying: see item #8 above portion: see item #9 above digital file: see item #2 above
50.	*transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output;*	transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output: see item #11 above portion: see item #9 above digital file: see item #2 above memory: see item #3 above
51.	*storing said first digital file portion* in said memory of said second device; and	storing said first digital file portion: Storing the "at least a portion" which was transferred to the second device, of the Digital File received in the "receiving" step (as opposed to a copy of the Digital File). digital file: see item #2 above portion: see item #9 above memory: see item #3 above
52.	rendering said first digital file portion through said output.	rendering: see item #25 above portion: see item #9 above digital file: see item #2 above This claim limitation's recitation of "said output" is inconsistent with the claim limitation "an audio and/or video output."

	'683 Claim 2	MS Construction
53.	2. A system including:	Claim as a Whole: The "system" is a VDE. (See item #93 for Microsoft's construction of VDE.)
54.	a first apparatus including,	
55.	user controls,	user controls: Controls created, modified, or selected by a user to Control a particular Use or Access by the user to particular Protected information. control: see item #17 above
56.	a communications port,	
57.	a processor,	
58.	a memory storing:	memory: see item #3 above
59.	a first secure container	secure container: A VDE Secure Container is a self-contained, self-protecting data structure which (a) encapsulates information of arbitrary size, type, format, and organization, including other, nested, containers, (b) cryptographically protects that information from all unauthorized Access and Use, (c) provides encrypted storage management functions for that information, such as hiding the physical storage location(s) of its protected contents, (d) permits the Association of itself or its contents with Controls and Control information Governing Access to and Use thereof, and (e) prevents such Use or Access (as opposed to merely preventing decryption) until it is "opened." A Secure Container can be opened only as expressly Allowed by the associated VDE Control(s), only within a Secure Processing Environment, and only through decryption of its encrypted header. A Secure Container is not directly accessible to any non-VDE or user calling process. All such calls are intercepted by VDE. The creator of a Secure Container can assign (or allow others to assign) control information to any arbitrary Portion of a Secure Container's contents, or to an empty Secure Container (to Govern the later addition of contents to the container, and Access to or Use of those contents). A container is not a Secure Container merely because its contents are encrypted and signed. A Secure Container is itself Secure. All VDE-Protected information (including protected content, information about content usage, content-control information, Controls, and Load Modules) is encapsulated within a Secure Container whenever stored outside a Secure Processing Environment or Secure Database.
60.	containing a governed item,	containing: Physically (directly) storing within, as opposed to Addressing. governed item: Information, of arbitrarily fine granularity, whose Access and Use by any user, process, or device is Controlled.
61.	the first secure container governed item being at least in part encrypted;	secure container: see item #59 above governed item: see item #60 above
62.	the first secure container having been received from a second apparatus;	the first secure container having been received from a second apparatus: The "first secure container" must Identify the single apparatus from which it was received, and that apparatus must be different from the first apparatus. Alternatively, if the Court does not construe this claim language as requiring the "first secure container" to identify the single apparatus from which it was received: This claim language has no patentable weight. It recites a step taken in the creation of the recited system, not a structural or functional characteristic of the system. One studying a particular system (as opposed to the process by which it was created) to compare it to the claimed system, could not distinguish a Secure Container received from another apparatus from, e.g., a Secure Container created on the first apparatus, and thus could not determine whether this step was satisfied.

	'683 Claim 2	MS Construction
		Receiving the Secure Container includes Authenticating the intended recipient in accordance with VDE Controls Associated With the Secure Container. The first Secure Container may be received as bar codes in a fax transmission, or filled ovals on a form delivered through physical mail. secure container: see item #59 above
63.	a first secure container rule	secure container rule: A Rule that Governs a Secure Container Governed Item. rule: A lexical statement that states a condition under which Access to or Use of VDE-Protected data will be Allowed by a VDE Control. A rule may specify how, when, where, and by whom a particular activity on particular information is to be Allowed.
64.	at least in part governing *an aspect of access to or use of* said first secure container governed item,	an aspect of access to or use of: Any one (as opposed to more than one) aspect of any Access to or (as opposed to "and") Use by any and all processes, users, and devices. governing: see Control (v.) item #7 above aspect: An aspect of an environment is a persistent element or property of that environment that can be used to distinguish it from other environments. access: see item #29 above use: To use information is to perform some action on it or with it (e.g., copying, printing, decrypting, encrypting, saving, modifying, observing, or moving, etc.). In VDE, information Use is Allowed only through execution of the applicable VDE Control(s) and satisfaction of all requirements imposed by such execution.
65.	the first secure container rule, *the first secure container rule having been received from a third apparatus different from said second apparatus;* and	the first secure container rule having been received from a third apparatus different from said second apparatus: The "first secure container rule" must have been encapsulated within a VDE Secure Container, and the intended recipient must have been Authenticated in accordance with VDE Controls Associated With the Secure Container, and the "first secure container rule" must have been accepted by the first apparatus. The "first secure container rule" must identify the single apparatus from which it was received, and that apparatus must be different from the first apparatus. Alternatively, if the Court does not construe this claim language as requiring the "first secure container" to identify the single apparatus from which it was received: This claim language has no patentable weight. It recites a step taken in the creation of the recited system, not a structural or functional characteristic of the system. One studying a particular system (as opposed to the process by which it was created) to compare it to the claimed system, could not distinguish a Secure Container Rule received from another apparatus from, e.g., a Secure Container Rule created on the first apparatus, and thus could not determine whether this step was satisfied. secure container rule: see item #63 above
66.	*hardware or software used for receiving and opening secure containers,*	hardware or software used for receiving and opening secure containers, receiving: This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites an undefined mechanism ("hardware or software") for performing a function (e.g., "Opening") without reciting particular structure that performs that function. The specification does not clearly link any particular structure to this recited function. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b). The recited function requires: the same single logical piece of either hardware or software (as opposed to both) must be capable of both receiving and Opening Secure

	'683 Claim 2	MS Construction
		Containers, this "receiving" including authenticating the intended recipient in accordance with VDE Controls Associated With the Secure Container, and this "Opening" performed by executing VDE Control(s) within VDE Secure Processing Environment(s). opening secure containers: Establishing the requisites needed to attempt to access the contents of a Secure Container. Opening is a necessary but insufficient step before the contents of a Secure Container may be copied, decrypted, read, manipulated, or otherwise Used, or Accessed. No process, user, or device may Access or Use the contents of a Secure Container without first opening that Secure Container. A Secure Container may be opened only through execution of the assigned VDE Control(s) within a VDE Secure Processing Environment and satisfaction of all requirements imposed by such execution.
67.	said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers;	said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers: Each Secure Container referred to in the phrase "hardware or software used for receiving and opening secure containers" must have the capacity to Contain a Governed Item, and must have Associated With it a Secure Container Rule. By "each secure container referred to in the phase ...," is meant each Secure Container which the "hardware or software used for receiving and opening secure containers" is capable of receiving and Opening. The Secure Container Rule is Associated With the Secure Container itself, as opposed to a Governed Item. secure container: see #59 above capacity: Available storage space that is still capable of allocation. For example, a 650 MB blank CD, after sealing, has zero capacity because no new material may be stored within it. contain: see item #60 above governed item: see item #60 above secure container rule: see item #63 above associated with: see item #4 above
68.	a protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus,	protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus: A single VDE Secure Processing Environment, in addition to and not within the first apparatus, actively Preventing (not merely being capable of Preventing, and not merely resisting) any "user" of the first apparatus from Tampering with any and all information encapsulated by the Secure Processing Environment (as opposed to Tampering with the Secure Processing Environment itself). Other components may or may not provide part of this Protecting function. The Protecting function is provided by use of the disclosed "Component Assembly" (VDE Controls), "Secure Container," "Protected Processing Environment," "object registration," and other mechanisms of the purported "VDE" "invention" for allegedly individually ensuring the "Access Control" "handcuffs" between specific "Controls," specific "objects" (and their content at an arbitrary granular level), and specific "users." protected processing environment: A uniquely identifiable, self-contained computing base trusted by all VDE nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the February, 1995, patent application as being protected, and to guarantee that such information will be accessed and used only as expressly authorized by VDE Controls. At most VDE nodes, the Protected

		'683 Claim 2	MS Construction
			Processing Environment is a Secure Processing Environment which is formed by, and requires, a hardware Tamper Resistant Barrier encapsulating a special-purpose Secure Processing Unit having a processor and internal secure Memory. ("Encapsulated" means hidden within an object so that it is not directly accessible but rather is accessible only through the object's restrictive interface.) The barrier prevents all unauthorized (intentional or accidental) interference, removal, observation, and Use of the information and processes within it, by all parties (including all users of the device in which the Protected Processing Environment resides), except as expressly authorized by VDE Controls. A Protected Processing Environment is under Control of Controls and control information provided by one or more parties, rather than being under Control of the appliance's users or programs. Where a VDE node is an established financial Clearinghouse, or other such facility employing physical facility and user-identity Authentication Security procedures trusted by all VDE nodes, and the VDE node does not Access or use VDE-protected information, or assign VDE control information, then the Protected Processing Environment at that VDE node may instead be formed by a general-purpose CPU that executes all VDE "security" processes in Protected (privileged) mode. A Protected Processing Environment requires more than just verifying the integrity of Digitally Signed Executable programming prior to execution of the programming; or concealment of the program, associated data, and execution of the program code; or use of a password as its protection mechanism. protecting: Maintaining the Security of. contain (contained): see item #60 above
69.		said protected processing environment including *hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container,* and	hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container: This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites an undefined mechanism ("hardware or software") for performing a function ("applying ... in combination") without reciting particular structure that performs that function. The specification does not clearly link any particular structure to this recited function. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b). The recited function requires: a single logical piece of either hardware or software (as opposed to both) to apply the two separate Rules in combination by assembling and executing a single Control, and to Govern any one or more aspects of any Access or Use by any process or user or device, of a Governed Item Contained in a Secure Container (which may or may not be any "Secure Container" recited earlier). Other components may or may not provide part of the Governing function. This "hardware or software" performs its functions by executing VDE Control(s) within VDE Secure Processing Environment(s). including: see item #2 above aspect: see item #64 above access: see item #29 above contain (contained): see item #60 above secure container rule: see item #63 above secure container: see #59 above

	'683 Claim 2	MS Construction
		governed item: see item #60 above
70.	*hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.*	hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses: This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites an undefined mechanism ("hardware or software") for performing a function (e.g., "transmission") without reciting particular structure that performs that function. The specification does not clearly link any particular structure to this recited function. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b). The recited function requires: a single logical piece of either hardware or software (as opposed to both) is capable of both transmission and receipt of Secure Containers, this receipt including Authenticating the intended recipient in accordance with VDE Controls Associated With the Secure Container. This "hardware or software" is separate from and in addition to the first apparatus, the recited "protected processing environment," and the recited "hardware or software used for receiving and opening secure containers." The transmission and receipt of the Secure Containers may be via bar codes in a fax transmission, or filled ovals on a form delivered through physical mail. This "hardware or software" performs its functions by executing VDE Control(s) within VDE Secure Processing Environment(s). secure container: see #59 above

	'721 Claim 1	MS Construction
71.	1. A security method comprising:	Claim as a whole: The recited method is performed within a VDE. (See item #93 for Microsoft's construction of VDE.)
72.	*digitally signing a first load module with a first digital signature designating the first load module for use by a first device class;*	digitally signing a first load module with a first digital signature designating the first load module for use by a first device class: Digitally Signing a particular ("first") Load Module by using a first Digital Signature as the signature Key, which signing indicates to any and all devices in the first device class that the signor authorized and restricted this Load Module for Use by that device. No VDE device can perform any execution of any Load Module without such authorization. The method ensures that the Load Module cannot execute in a particular device class and ensures that no device in that device class has the Key(s) necessary to verify the Digital Signature. digital signature: digital signature: A computationally unforgeable string of characters (e.g., bits) generated by a cryptographic operation on a block of data using some secret. The string can be generated only by an Entity that knows the secret, and hence provides evidence that the Entity must have generated it. digitally signing: Creating a Digital Signature using a secret Key. (In symmetric key cryptography, a "secret key" is a Key that is known only to the sender and recipient. In asymmetric key cryptography, a "secret key" is the private Key of a public/private key pair, in which the two keys are related uniquely by a predetermined mathematical relationship such that it is computationally infeasible to determine one from the other.) load module: An Executable, modular unit of machine code (which may include data) suitable for loading into Memory for execution by a processor. A Load Module is encrypted (when not within a secure processing unit) and has an Identifier that a calling process must provide to be able to use the Load Module. A Load Module is combinable with other Load Modules, and associated data, to form Executable Component Assemblies. A Load Module can execute only in a VDE Protected Processing Environment. Library routines are not Load Modules and dynamic link libraries are not Load Modules. designating: Designating something for a particular Use means specifying it for and restricting it to that Use. use: see item #64 above device class: The generic name for a group of device types. For example, all display stations belong to the same device class. A device class is different from a device type. A device type is composed of all devices that share a common model number or family (e.g. IBM 4331 printers).
73.	*digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security*	digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class: Digitally Signing a different ("second") Load Module by using a different ("second") Digital Signature as the signature Key, which signing indicates to any and all devices in the second device class that the signor authorized and restricted this Load Module for Use by that device. No VDE device can perform any execution of any Load Module without such authorization. The method ensures that the Load Module cannot execute in a particular device class and ensures that no device in that device class has the Key(s) necessary to verify the Digital Signature. All devices in the first device class have the same persistent (not just occasional) and identified level of Tamper Resistance and the same persistent and identified Level of Security. All devices in the second device class have the same persistent and

		'721 Claim 1	MS Construction
		level of the first device class;	identified level of Tamper Resistance and same persistent and identified Level of Security. The identified level of Tamper Resistance or identified Level of Security (or both) for the first device class, is greater than or less than the identified Level Of Tamper Resistance or identified Level of Security for the second device class. . digital signature: see item #72 above designating: see item #72 above device class: see item #72 above load module: see item #72 above use: see item #64. level of security: An ordered measure of the degree of trustworthiness. The "security level" is persistent unless expressly noted to exist only some of the time. Also, the combination of a hierarchical classification and a set of nonhierarchical categories that represents the sensitivity of an object or the clearance of a subject. For example, Unclassified, Confidential, Secret, and Top Secret are hierarchical classifications, whereas NATO and NOFORN are non-hierarchical categories defined by the Department of Defense Trusted Computing guidelines. tamper resistance: The ability of a Tamper Resistant Barrier to prevent Access, observation, and interference with information or processing encapsulated by the barrier.
74.		*distributing the first load module for use by at least one device in the first device class;* and	distributing the first load module for use by at least one device in the first device class: The first Load Module, Digitally Signed as indicated above, is transmitted to at least one device in the first device class. load module: see item #72 above device class: see item #72 above
75.		*distributing the second load module for use by at least one device in the second device class.*	distributing the second load module for use by at least one device in the second device class: The second Load Module, Digitally Signed as indicated above, is transmitted to at least one device in the second device class. load module: see item #72 above device class: see item #72 above

	'721 Claim 34	MS Construction
76.	34. A protected processing environment comprising:	Claim as a Whole: The "Protected Processing Environment" is part of and within VDE. (See item #93 for Microsoft's construction of VDE.)
77.	a first tamper resistant barrier having a first security level,	tamper resistant barrier: An active device that encapsulates and separates a Protected Processing Environment from the rest of the world. It prevents information and processes within the Protected Processing Environment from being observed, interfered with, and leaving except under appropriate conditions ensuring Security. It also Controls external access to the encapsulated Secure resources, processes and information. A Tamper Resistant Barrier is capable of destroying protected information in response to Tampering attempts. security level: see item #73 above
78.	a first secure execution space, and	secure execution space: An allocated Portion of the Secure Memory within a special-purpose secure processing unit which is isolated from the rest of the world, and protected from observation by (and encapsulated within) a Tamper Resistant Barrier and protected from alteration by the processor. The processor cryptographically verifies the integrity of all code loaded from Secure Memory prior to execution, executes only the code that the processor has authenticated for its use, and is otherwise Secure.
79.	at least one *arrangement within the first tamper resistant barrier* that	arrangement within the first tamper resistant barrier: An organization of hardware and software which arrangement is located and executed wholly within the first Tamper Resistant Barrier. arrangement: A collection of things that have been arranged. In context, the term requires an organization of hardware and software and data, or hardware and software, or hardware and data. tamper resistant barrier: see item #72 above
80.	*prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level.*	prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level: "A second secure execution space having a second tamper resistant barrier with a second security level different from the first security level": a second Secure Execution Space (different from the first Secure Execution Space) is part of the Protected Processing Environment, and has a Tamper Resistant Barrier (different from the first Tamper Resistant Barrier) that has a persistent (not just occasional) Security Level greater than or less than the first persistent Security Level. "The same executable accessed by": the same Executable (as opposed to, e.g., two copies of the same Executable) is simultaneously accessed by both the first Secure Execution Space and the second Secure Execution Space. "Prevents the first secure execution space from executing": the arrangement Prevents the first Secure Execution Space, otherwise capable of executing the Executable, from executing any part of the Executable (e.g., on behalf of any user, process, or device). prevents: Imposes an active restraint on an action such that it cannot occur by any means or under any circumstances. access (accessed): see item #29 above security level: see item #73 above

| | | secure execution space: see item #78 above |
| | | tamper resistant barrier: see item #72 above |

	'861 Claim 58	MS Construction
81.	58. A method of	<u>Claim as a whole</u>: The recited method is performed within a VDE. (See item #93 for Microsoft's construction of VDE.)
82.	*creating a first secure container*, said method including the following steps;	<u>creating a first secure container</u>: This preamble language is a claim limitation. Completely forming (as opposed to defining) the Secure Container, within a VDE Secure Processing Environment(s). <u>secure container</u>: see item #59 above
83.	accessing a descriptive data structure, said descriptive data structure *including or addressing organization information at least in part describing a required or desired organization of a content section of said first secure container, and metadata information at least in part specifying at least one step required or desired in creation of said first secure container;*	<u>including or addressing organization information at least in part describing a required or desired organization of a content section of said first secure container, and metadata information at least in part specifying at least one step required or desired in creation of said first secure container</u>: The same single Descriptive Data Structure must either Contain within its confines or Address both Organization Information and Metadata Information. Both the "desired" organization of the content section and also the "desired" step, occur after the Descriptive Data Structure is accessed, not before. The Metadata Information explicitly dentifies a procedure ("step") that must be executed in creation of the first Secure Container, as opposed to Iidentifying a procedure to be run if later required or desired, as opposed to Identifying a result or a Data Item to be included in the first Secure Container, and as opposed to identifying information which operates as a parameter for a procedure. <u>required</u>: A condition without which an action cannot occur. A required condition acts prospectively – it does not apply to a description created at or after the creation of the object to which it applies. <u>access</u> (accessing): see item #29 above <u>descriptive data structure</u>: A machine-readable data structure (e.g., text file, template, etc.) Containing or Addressing descriptive information (e.g., Metadata, shorthand abstract representation, integrity constraints, Rules, instructions, etc.) about (1) the layout, generic format, attributes, or hierarchical structure of the contents section of one or a family of other data structure(s) (e.g., a rights management data structure), (2) the operations or processes used to create or Use such other data structure(s), and/or (3) the consequences of such operations. The Descriptive Data Structure is capable of being used to create or handle (e.g., read, locate information within, request information from, and/or manipulate) the other data structure(s). The Descriptive Data Structure is not Associated With the other data structure(s) and does not Contain or specify its particular contents (e.g., "Yankees Win the Pennant!"). <u>addressing</u>: Referring to something by the specific location where it is stored, without directly storing it. The location is explicitly identified by its name or number. <u>Organization</u> (organization, organization information): The manner in which data is represented and laid out in physical storage. For example, for data organized as records: the field hierarchy, order, type and size. organize: Representing and laying out data in a particular manner in physical storage. <u>metadata information</u>: Information that describes one or more attributes of other data, and/or the processes used to create and/or Use that data. For example, Metadata Information may describe the following attributes of other data: its meaning, representation in storage, what it is used for and by whom, context, quality and condition, location, ownership, or its data elements or their attributes (name, size, data

	'861 Claim 58	MS Construction
		type, etc.)
84.	using said descriptive data structure to organize said first secure container contents;	descriptive data structure: see item #83 above including: see item #2 above organize: see item #83 above
85.	using said metadata information to *at least in part determine specific information required to be included in said first secure container contents*; and	at least in part determine specific information required to be included in said first secure container contents: The Metadata Information is used to determine the specific value, not merely the kind, of at least some of the information that must be placed inside the Secure Container. The use of the Metadata Information actively requires the Secure Container creation steps to add this specific information to the first Secure Container, as opposed to the specific information being within the Secure Container for some other reason. required: see item #83 above including (included): see item #2 above
86.	*generating or identifying at least one rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents.*	generating or identifying at least one rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents: Generating or Identifying Rule designed for these particular Secure Container contents, which is used (by VDE Control(s) executing in VDE Secure Processing Environment(s)) to limit Access to or Use of at least a Portion of the contents of the first Secure Container (by all users, processes, and devices). Without compliance with this Rule, no process, user, or device is able to take the Controlled aspect of the Controlled Access or Use action. The Rule is generated or Identified based at least in part on the Descriptive Data Structure. generating: Producing. identifying: see item #19 above rule: see item #63 above control: see item #17 above aspect: see item #64 above access: see item #29 above use: see item #43 above portion: see item #9 above secure container: see item #59 above

		'891 Claim 1	MS Construction
87.		1. A method for using at least one	**Claim as a whole**: The recited method is performed within a VDE. (See item #93 for Microsoft's construction of VDE.)
88.		*resource processed in a secure operating environment at a first appliance*, said method comprising:	**resource processed in a secure operating environment at a first appliance**: This preamble language is a claim limitation. A shared facility, required by a job or task, of a first appliance's Secure Operating Environment which is processed within that Secure Operating Environment's special-purpose Secure Processing Unit. A Secure Processing Unit is a special-purpose unit isolated from the rest of the world in which a hardware Tamper Resistant Barrier encapsulates a processor and internal Secure Memory. The Tamper Resistant Barrier prevents all unauthorized interference, removal, observation, and Use of the information and processes within it. The processor cryptographically verifies the integrity of all code loaded from the Secure Memory prior to execution, executes only the code that the processor has authenticated for its Use, and is otherwise Secure. **resource processed**: A record containing control information, which record is stored and acted upon within a processing environment. **secure operating environment**: Same as Secure Processing Environment.
89.		*securely receiving a first entity's control at said first appliance*, said first entity being located remotely from said operating environment and said first appliance;	**securely receiving a first entity's control at said first appliance**: This claim language falls within 35 U.S.C. § 112, ¶ 6. It recites a step or result ("Securely receiving") without reciting an action that achieves that result. The specification does not clearly link any particular action to this recited step. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b). The recited function requires: A first appliance obtaining a VDE Secure Container encapsulating a Control created, selected, or modified by a first entity, as part of a communication encrypted on the communications level, authenticating the first appliance in accordance with VDE Controls Associated With the Secure Container, and accepting the Secure Container. **entity**: Any person or organization. **entity's control**: Control created, modified, or selected by any person or organization to Control a particular Use of or Access to particular Protected information by a particular user(s). **control**: see item #17 above **operating environment**: see item #88 above
90.		*securely receiving a second entity's control at said first appliance*, said second entity being located remotely from said operating environment and said first appliance, said second entity being different from said first entity; and	**securely receiving a second entity's control at said first appliance**: This claim language falls within 35 U.S.C. § 112, 6. It recites a step or result ("securely receiving") without reciting an action that achieves that result. The specification does not clearly link any particular action to this recited step. Part of the recited function is performed by Communications Controller 666, I/O Controller 600, SPE 503/SPU 500 (particularly "SPU Encryption/Decryption Engine 522" and NVRAM 534b). The recited function requires: A first appliance obtaining a VDE Secure Container encapsulating a Control created, selected, or modified by a second entity, as part of a communication encrypted on the communications level, Authenticating the first appliance in accordance with VDE Controls Associated With the Secure Container, and accepting the Secure Container.

	'891 Claim 1	MS Construction
		entity's control: see item #89 above control: see item #17 above
91.	*securely processing a data item at said first appliance, using at least one resource, including*	securely processing a data item at said first appliance, using at least one resource, including : Performing an operation, inside the special-purpose Secure Processing Unit of the first appliance, on a Data Item inside the Secure Processing Unit. The operation cannot be observed from outside the Secure Processing Unit and is performed only after the integrity of the program code for performing such operation is cryptographically verified. A Secure Processing Unit is a special-purpose unit isolated from the rest of the world in which a hardware Tamper Resistant Barrier encapsulates a processor and internal Secure Memory. The Tamper Resistant Barrier prevents all unauthorized interference, removal, observation, and Use of the information and processes within it. The processor cryptographically verifies the integrity of all code loaded from the Secure Memory prior to execution, executes only the code that the processor has authenticated for its Use, and is otherwise Secure. control: see item #17 above data item: An individual unit of digital information representing a single value, such as that stored in a field of a larger Record in a database. It is the smallest useful unit of named information in the system. resource: A shared facility of a computing system or operating system, which is required by a job or task, and is processed by a processing unit.
92.	*securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item.*	securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item: Processing the resource (component part of a first appliance's Secure Operating Environment) within the Secure Operating Environment's special-purpose Secure Processing Unit to execute the first Control and second Control in combination within the Secure Processing Unit. This execution of these Controls Governs all Use of the Data Item by all users, processes, and devices. The processing of the Resource and execution of the Controls cannot be observed from outside the Secure Processing Unit and is performed only after the integrity of the Resource and Controls is cryptographically verified. A Secure Processing Unit is a special-purpose unit isolated from the rest of the world in which a hardware Tamper Resistant Barrier encapsulates a processor and internal Secure Memory. The Tamper Resistant Barrier prevents all unauthorized interference, removal, observation, and Use of the information and processes within it. The processor cryptographically verifies the integrity of all code loaded from the Secure Memory prior to execution, executes only the code that the processor has authenticated for its Use, and is otherwise Secure. control: see item #17 above data item: see item #91 above resource: see item #91 above use: see item #43 above govern: see Control (v.) item #7 above

	'900 Claim 155	MS Construction
93.	155. A virtual distribution environment comprising	**Claim as a Whole:** The "virtual distribution environment" is VDE. **VDE/Virtual Distribution Environment:** **Data Security and Commerce World:** InterTrust's February 13, 1995, patent application described as its "invention" a **Virtual Distribution Environment** ("**VDE invention**") for Securing, administering, and auditing all Security and commerce digital information within its multi-node world (community). VDE guarantees to all VDE "participants" identified in the patent application that it will limit all **Access** to and **Use** (i.e., interaction) of such information to **Authorized** activities and amounts, will ensure any requested reporting of and payment for such **Use**, and will maintain the availability, secrecy, integrity, non-repudiation and authenticity of all such information present at any of its nodes (including **Protected** content, information about content usage, and content **Controls**.). VDE is Secure against at least the threats identified in the Feburary 1995, patent application to this availability (no user may delete the information without **Authorization**), secrecy (neither available nor disclosed to unauthorized persons or processes), integrity (neither intentional nor accidental alteration), non-repudiation (neither the receiver can disavow the receipt of a message nor can the sender disavow the origination of that message) and authenticity (asserted characteristics are genuine). VDE further provides and requires the components and capabilities described below. Anything less than or different than this is not VDE or the described "invention." **Secure Processing Environment:** At each node where VDE-Protected information is Accessed, Used, or assigned control information, VDE requires a **Secure Processing Environment.** A Secure Processing Environment is uniquely identifiable, self-contained, non-circumventable, and trusted by all other VDE nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the patent application as being **Protected**, and to guarantee that such information will be **Accessed** and **Used** only as expressly **Authorized** by the associated **VDE Controls**, and to guarantee that all requested reporting of and payments for protected information use will be made. A Secure Processing Environment is formed by, and requires, a Secure Processing Unit having a hardware **Tamper Resistant Barrier** encapsulating a processor and internal **Secure Memory**. The **Tamper Resistant Barrier** prevents all unauthorized interference, removal, observation, and other **Use** of the information and processes within it. **VDE Controls:** VDE Allows Access to or Use of Protected information and processes only through execution of (and satisfaction of the requirements imposed by) independent, special-purpose, **Executable VDE Control(s).** Each VDE Control is a **Component Assembly** dedicated to a particular activity (e.g., editing, modifying another Control, a user-defined action, etc.), particular user(s), and particular protected information. Each separate information **Access** or **Use** is independently **Controlled** by independent VDE Control(s). A VDE Control can execute only within a Secure Processing Environment. Each VDE Control is assembled, within a Secure Processing Environment, from independently deliverable modular components (e.g., **Load Modules** or other **Controls**), dynamically in response to an information Access or Use request. The dynamic assembly of a Control is directed by a "blueprint" **Record** (put in place by one or more VDE users) **Containing** control information identifying the exact modular code components to be assembled and executed to **Govern** this particular activity on this particular information by this particular user(s). Each **Control** is independently assembled, loaded and delivered vis-à-vis other **Controls**. Control information and **Controls** are extensible and can be configured and modified by all users, and combined by all users with any other VDE control information or **Controls** (including that provided by other users), subject only to "senior" user **Controls**. Users can assign control information and **Controls** to all of or an arbitrarily fine, user-defined **Portion** of the **Protected** information, such as a single paragraph of a document, as opposed to being limited to file-based controls.

	'900 Claim 155	MS Construction
		VDE Controls reliably limit Access and Use of the protected information to Authorized activities and amounts.
		VDE Secure Container: A VDE Secure Container is a self-contained, self-protecting data structure which (a) encapsulates information of arbitrary size, type, format, and organization, including other, nested, containers, (b) cryptographically protects that information from all unauthorized Access and Use, (c) provides encrypted storage-management functions for that information, such as hiding the physical storage location(s) of its Protected contents, (d) permits the Association of itself and/or all of or arbitrary Portions of its contents with Controls and control information Governing Access to and Use thereof, and (e) Prevents such Use or Access (as opposed to merely Preventing decryption) until it is opened. A Secure Container Can Be opened only as expressly Allowed by the associated VDE Control(s), only within a Secure Processing Environment, and only through decryption of its encrypted header. A Secure Container is not directly accessible to any non-VDE calling process. All such calls are intercepted by VDE. The creator of a Secure Container can assign (or allow others to assign) control information to all of or any arbitrary Portion of a Secure Container's contents, or to an empty Secure Container (to Govern the addition of contents to the Secure Container, and Access to or Use of those contents). A container is not a Secure Container merely because its contents are encrypted and signed. All VDE-Protected information (including protected content, information about content usage, and Controls) is encapsulated within a Secure Container whenever stored outside a Secure Processing Environment or Secure Database.
		Non-Circumventable: VDE is non-circumventable (sequestered). It intercepts all attempts by any and all users, processes, and devices, to Access or Use, such as observing, interfering with, or removing) Protected information, and Prevents all such attempts other than as Allowed by execution of (and satisfaction of all requirements imposed by) Associated VDE Controls within Secure Processing Environment(s).
		Peer to Peer: VDE is peer-to-peer. Each VDE node has the innate ability to perform any role identified in the patent application (e.g., end user, content packager, distributor, Clearinghouse, etc.), and can protect information flowing in any direction between any nodes. VDE is not client-server. It does not pre-designate and restrict one or more nodes to act solely as a "server" (a provider of information (e.g., authored content, control information, etc.) to other nodes) or "client" (a requestor of such information). All types of protected-content transactions can proceed without requiring interaction with any server.
		Comprehensive Range of Functions: VDE comprehensively Governs all Security and commerce activities identified in the patent application, including (a) metering, budgeting, monitoring, reporting, and auditing information usage, (b) billing and paying for information usage, and (c) negotiating, signing and enforcing contracts that establish users' rights to Access or Use information.
		User-Configurable: The specific protections Governing specific VDE-Protected information are specified, modified, and negotiated by VDE's users. For example, VDE enables a consumer to place limits on the nature of content that may be accessed at her node (e.g., no R-rated material) or the amount of money she can spend on viewing certain content, both subject only to other users' senior Controls.
		General Purpose; Universal: VDE is universal as opposed to being limited to or requiring any particular type of appliance, information, or commerce model. It is a single, unified standard and environment within which an unlimited range of electronic rights protection, data Security, electronic currency, and banking applications can run.
		Flexible: VDE is more flexible than traditional information Security and commerce

	'900 Claim 155	MS Construction
		systems. For example, VDE allows consumers to pay for only the user-defined Portion of information that the user actually uses, and to pay only in proportion to any quantifiable VDE event (e.g., for only the number of paragraphs displayed from a book), and allows editing the content in VDE containers while maintaining its Security.
94.	a first host processing environment comprising	a first host processing environment comprising: A Host Processing Environment that encompasses the recited computer hardware (central processing unit, main Memory, and mass storage) and certain VDE Protected Processing Environment software loaded in that main Memory and executing in that central processing unit, but does not encompass software, such as the recited Tamper Resistant Software, which is stored in mass storage and not executing. host processing environment: A processing environment within a VDE node which is not a Secure Processing Environment. A "host processing environment" may either be "secure" or "not secure." A "secure host processing environment" is a self-contained Protected Processing Environment, formed by loaded, Executable programming executing on a general purpose CPU (not a Secure Processing Unit) running in protected (privileged) mode. A "non-secure host processing environment" is formed by loaded, Executable programming executing on a general purpose CPU (not a Secure Processing Unit) running in user mode.
95.	a central processing unit;	
96.	main memory operatively connected to said central processing unit;	memory: see item #3 above
97.	mass storage operatively connected to said central processing unit and said main memory;	memory: see item #3 above
98.	said mass storage storing tamper resistant software	said mass storage storing tamper resistant software: The Tamper Resistant Software is physically stored within, as opposed to being merely Addressed by, the mass storage. tamper resistant software: Software that is encapsulated and executed wholly within a Tamper Resistant Barrier.
99.	designed to be loaded into said main memory and executed by said central processing unit,	designed to be loaded into said main memory and executed by said central processing unit: The Tamper Resistant Software is capable of being loaded into only said main Memory and is capable of being executed only by said central processing unit.
100.	said tamper resistant software comprising: machine check programming which derives information from one or more aspects of said host processing environment, one or more storage locations storing said information;	said tamper resistant software comprising: machine check programming which derives information from one or more aspects of said host processing environment, one or more storage locations storing said information: The Tamper Resistant Software within said mass storage includes one or more storage locations within it. These storage locations are designated to store, and must store, information Derived by the Machine Check Programming, and must not store any other information. machine check programming: Executable programming that when executed checks a machine and generates a unique "machine signature" which distinguishes the physical machine from all other machines. This machine check programming code sometimes is invoked by integrity programming. host processing environment: see item #94 above

	'900 Claim 155	MS Construction
		derives: To retrieve from a specified source. aspect: see item #64 above
101.	derives information from one or more aspects of said host processing environment	derives information from one or more aspects of said host processing environment: Deriving from the Host Processing Environment hardware one or more values that uniquely and persistently Identify the Host Processing Environment and distinguish it from other Host Processing Environments. The "one or more aspects of said host processing environment" are persistent elements or properties of the Host Processing Environment itself that are capable of being used to distinguish it from other environments, as opposed to, e.g., data or programs stored within the mass storage or main Memory, or processes executing within the Host Processing Environment. host: see item #94 above derives: see item #100 above aspect: see item #64 above
102.	one or more storage locations storing said information;	One or more storage locations: One or more logical storage locations within the Tamper Resistant Software storing only information Derived by the Machine Check Programming.
103.	integrity programming which causes said machine check programming to derive said information, compares said information to information previously stored in said one or more storage locations, and	integrity programming: Executable programming that when executed checks and reports on the integrity of a device or process. "Integrity" means the property that information has not been altered either intentionally or accidentally. information previously stored in said one or more storage locations: Any information once stored in said "one or more storage locations storing said information," but not stored therein when the recited comparison occurs. information previously stored: Information that once was stored but is no longer stored. derive: see item #100 above compares: A processor operation that evaluates two quantities and sets one of three flag conditions as a result of the comparison – greater than, less than, or equal to.
104.	generates an indication based on the result of said comparison; and	generates an indication based on the result of said comparison: Producing an indication based on the result of the "compares" step. The "indication" need not be displayed to a user. The indication is based solely on that result. There are only two possible indications: exact match found or exact match not found. comparison: see item #103 above
105.	programming which takes one or more actions based on the state of said indication;	programming which takes one or more actions based on the state of said indication: Executable programming code that is a part of the Tamper Resistant Software, when executed, and not a part of the Host Processing Environment. Whenever the recited indication is generated, no matter what it indicates, this code (executing on the CPU for which it was designed and loaded in the Memory for which it was designed) must take an action, or more than one action. The particular action(s) taken must be based

	'900 Claim 155	MS Construction
		solely on the state of that indication.
106.	said one or more actions including *at least temporarily halting further processing*.	at least temporarily halting further processing: The action(s) taken by this programming must encompass Halting or temporarily Halting all further processing of the Host Processing Environment and any processes running within it. halting: Stopping execution of a running (executing) process unconditionally (i.e., without providing any specific condition for resumption). For example, executing an instruction known as a "breakpoint halt instruction."

	'912 Claim 8	MS Construction
107	8. A process comprising the following steps:	<u>Claim as a whole</u>: The recited method is performed within a VDE. (See item #93 for Microsoft's construction of VDE.)
108	accessing a first record containing information directly or indirectly identifying one or more elements of a first component assembly,	<u>record</u>: A data structure that is a collection of fields (elements), each with its own name and type. Unlike an array, whose elements are accessed using an index, the elements of a record are accessed by name. A record can be accessed as a collective unit of elements, or the elements can be accessed individually. <u>identifying</u>: see item #19 above <u>access</u>: see item #29 above <u>comparison</u>: see item #103 above <u>component assembly</u>: A cohesive Executable component created by a channel which binds or links together two or more independently deliverable Load Modules, and Associated data. A Component Assembly is assembled, and executes, only within a VDE Secure Processing Environment. A Component Assembly is assembled dynamically in response to, and to service, a particular content-related activity (e.g., a particular Use request). Each VDE Component Assembly is assigned and dedicated to a particular activity, particular user(s), and particular Protected information. Each Component Assembly is independently assembled, loadable and deliverable vis-à-vis other Component Assemblies. The dynamic assembly of a Component Assembly is directed by a "blueprint" Record Containing Control information for this particular activity on this particular information by this particular user(s). Component Assemblies are extensible and can be configured and reconfigured (modified) by all users, and combined by all users with other Component Assemblies, subject only to other users' "senior" Controls.
109	at least one of said elements including at least some executable programming,	<u>executable programming</u>: Executable: A cohesive series of machine code instructions in a format that can be loaded into Memory and run (executed) by a connected processor. executable programming: A cohesive series of machine code instructions, comprising a computer program, in a format that can be loaded into Memory and run (executed) by a connected processor. (A "computer program" is a complete series of definitions and instructions that when executed on a computer will perform a required or requested task.) <u>including</u>: see item #2 above
110	at least one of said elements constituting a load module,	<u>load module</u>: see item #72 above
111	said load module including executable programming and a header;	<u>load module</u>: see item #72 above <u>including</u>: see item #2 above <u>executable programming</u>: see item #109 above
112	said header including an execution space identifier *identifying at least one aspect of an execution space required for use*	<u>identifying at least one aspect of an execution space required for use and/or execution of the load module</u>: Defining fully, without reference to any other information, at least one of the persistent elements or properties (aspects) (that are capable of being used to distinguish it from other environments of an Execution Space) that are Required for any Use, and/or for any execution, of the Load Module. An Execution Space without

EXHIBIT A TO JOINT CLAIM CONSTRUCTION STATEMENT

	'912 Claim 8	MS Construction
	and/or execution of the load module associated with said header;	all of those Required aspects is incapable of making any such execution and/or other Use (e.g., Copying, displaying, printing) of the Load Module. including: see item #2 above execution space identifier: A value that uniquely identifies a particular execution space. execution space: A processor-addressable physical Memory into which data and Executable code can be loaded, which is assigned to a single executing process while that process is actively executing. Memory holding "swapped out" processes or Executables is not part of an "execution space." load module: see item 110 above required: see item #83 above aspect: see item #64 above associated with: see item #4 above identifying: see item #19 above
113	*said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security;*	said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security: The Execution Space Identifier, by itself, provides the Load Module with the capability of determining the persistent Level of Security of any Execution Space in which it is loaded, and of distinguishing between any two Execution Spaces based on their respective, determined persistent (not just occasional) "Levels Of Security." This capability extends to at least two Execution Spaces providing a higher Level of Security and at least two Execution Spaces providing a lower Level of Security. execution space identifier: see item #112 above execution space: see item #112 above level of security: see Security Level, item #73 above
114	using said information to identify and locate said one or more elements;	identify: see item #19 above
115	accessing said located one or more elements;	access: see item #29 above
116	securely assembling said one or more elements to form at least a portion of said first component assembly;	securely assembling: Securely (1) linking or binding plural distinct elements together in a particular manner (specified by authenticated assembly instructions) into a single cohesive Executable unit so the elements can directly reference each other element within the resulting assembly, within a VDE Secure Processing Environment, (2) validating and verifying the authenticity and integrity of each element (e.g., that it has not been modified from or substituted for the correct element) immediately prior to binding it into the assembly, and (3) ensuring that the elements are linked together only in ways that are intended by the VDE participants who created the elements and/or specified the assembly thereof. component assembly: see item #108 above
117	executing at least some of said executable programming; and	executable programming: see item #109 above

	'912 Claim 8	MS Construction
118.	*checking said record for validity prior to performing said executing step.*	checking said record for validity prior to performing said executing step: Before executing any Executable Programming encompassed within any element which is directly or indirectly identified by any information Contained within the first Record, evaluating, within a VDE Secure Processing Environment, the values and formats of all data fields within the first Record and confirming that they have legitimate values and formats. record: see item #108 above validity: The state in which authenticated data conforms to predetermined completeness and consistency parameters.

	'912 Claim 35	MS Construction
119.	35. A process comprising the following steps:	Claim as a whole: The recited method is performed within a VDE. (See item #93 for Microsoft's construction of VDE.)
120.	at a first processing environment receiving a first record from a second processing environment remote from said first processing environment;	processing environment: A standardized, well-defined, self-contained, computing base, formed by hardware and executing code, that provides an "interface" and set of resources which can support different applications, on different types of hardware platforms. In the context of claim 35 of the '912 patent: a Secure Processing Environment. record: see item #108 above
121.	said first record being *received in a secure container;*	received in a secure container: The first Processing Environment obtained a VDE Secure Container encapsulating the Record inside, and authenticated the intended recipient in accordance with VDE Controls Associated With the Secure Container, and accepted the Secure Container. secure container: see item #59 above
122.	said first record containing identification information directly or indirectly identifying one or more elements of a first component assembly;	containing: see item #60 above identifying: see item #19 above component assembly: see item #108 above
123.	at least one of said elements including at least some executable programming;	including: see item #2 above
124.	*said component assembly allowing access to or use of specified information;*	said component assembly allowing access to or use of specified information: The Component Assembly identifies specific information (the specific value, not merely the kind of information) over which it (by itself and with no other information), executing in a VDE Secure Processing Environment, Allows Access or Use (as opposed to Access "and" Use). Unless Allowed by the Component Assembly, no user, process, or device is able to Access or Use the specified information. The Component Assembly is Associated With and dedicated to this particular specified information. component assembly: see item #108 above allow (allowing): see item #10 above access: see item #29 above
125.	said secure container also including a first of said elements;	secure container: see item #59 above including: see item #2 above
126.	accessing said first record;	access: see item #29 above record: see item #108 above
127.	using said identification information to identify and locate said one or more elements;	identify: see item #19 above

EXHIBIT A TO JOINT CLAIM CONSTRUCTION STATEMENT
Page 36 of 37

128.	said locating step including locating a second of said elements at a third processing environment located remotely from said first processing environment and said second processing environment;	processing environment: see item #120 above
129.	accessing said located one or more elements;	access (accessing): see item #29 above
130.	said element accessing step including retrieving said second element from said third processing environment;	
131.	securely assembling said one or more elements to form at least a portion of *said first component assembly specified by said first record*; and	said first component assembly specified by said first record: The first Record by itself Contains sufficient information to unambiguously Identify the assembled Component Assembly, including all of its elements. This limitation is inconsistent with the recitation "first record containing identification information directly or indirectly identifying one or more elements of first component assembly." securely assembling: see item #116 above component assembly: see item #108 above record: see item #108 above
132.	executing at least some of said **executable programming,**	executable programming: see item #109 above
133.	said executing step taking place at said first processing environment.	processing environment: see item #120 above

Exhibit B

EXHIBIT B

PLR 4-3(a) – Constructions on Which the Parties Agree

Claim Term / Phrase	Agreed Construction
Entity 891.1	Any person or organization.
Generating 861.58	Producing.
Govern, governed, governing 891.1, 683.2	See Control (v.).
Metadata information 861.58	Information that describes one or more attributes of other data, and/or the processes used to create and/or use that data. For example, metadata information may describe the following attributes of other data: its meaning, representation in storage, what it is used for and by whom, context, quality and condition, location, ownership, or its data elements or their attributes (name, size, data type, etc.)
Rendering 193.11, 193.15, 193.19	In the context of 193.11, 15 and 19: Playing content through an audio output (e.g., speakers) or displaying content on a video output (e.g., a screen).
Secure container rule 683.2	A Rule that Governs a Secure Container Governed Item.
Security 721.1, 721.34	See Secure.
Tampering 683.2, 721.1, 721.34, 900.155	Using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use.
"said mass storage storing tamper resistant software" 900.155	The Tamper Resistant Software is physically stored within, as opposed to being merely Addressed by, the mass storage.
"including using said key to decrypt at least a portion of said first digital file" 193.19	The "at least one use of said digital file" must encompass decrypting at least a Portion of the Digital File using the Key.

Notation:
    Each term is followed by a list of the claims in which it appears (e.g., "193.15" means claim 15 from the '193 patent).
    '193 patent = U.S. Patent No. 6,253,193
    '683 patent = U.S. Patent No. 6,185,683
    '721 patent = U.S. Patent No. 6,157,721
    '891 patent = U.S. Patent No. 5,982,891
    '861 patent = U.S. Patent No. 5,920,861
    '912 patent = U.S. Patent No. 5,917,912
    '900 patent = U.S. Patent No. 5,892,900

PLR 4-3(b) – InterTrust's Construction of Disputed Terms & Phrases

Claim Term / Phrase	InterTrust Construction
access, accessed, access to, accessing 193.15, 193.19, 912.8, 912.35, 861.58, 683.2, 721.34	To obtain something so it can be used.
addressing 861.58	Referring by specific location or individual name to something without directly storing it.
allowing, allows 912.35, 193.1, 193.11, 193.15, 193.19	Normal English: permitting, permits; letting happen, lets happen.
arrangement 721.34	Normal English: a collection of things that have been arranged. In context, the term can apply to an organization of hardware and/or software and/or data.
aspect 900.155, 912.8, 861.58, 683.2	Feature, element, property or state.
associated with 912.8, 193.1, 193.11, 193.15, 683.2	Having a relationship with.
authentication 193.15	Identifying (e.g., a person, device, organization, document, file, etc.). Includes uniquely identifying or identifying as a member of a group.
authorization information, authorized, not authorized 193.15, 193.19	Authorize: Normal English: permit. Authorization Information: Information (e.g., a key) received if an action is Authorized. Information: nonaccidental signal(s) or character(s) used in a computer or communication system. Information includes programs and also includes data.
budget control; budget 193.1	Budget: Information specifying a limitation on usage. See Authorization Information for the definition of Information. Budget control: The term is explicitly defined in the claim as a Control "including a budget specifying the number of copies which can be made of said digital file."
can be 193.1	Normal English: the specified act is able or authorized to be carried out. In context, this means the number of copies allowed to be made.
capacity 683.2	Normal English: "ability," or "capability."
clearinghouse 193.19	A provider of financial and/or administrative services for a number of Entities; or an entity responsible for the collection, maintenance, and/or distribution of materials, information, licenses, etc.

Claim Term / Phrase	InterTrust Construction
compares, comparison 900.155	Normal English: Compares: examines for the purpose of noting similarities and differences. Comparison: the act of comparing.
component assembly 912.8, 912.35	Components are code and/or data elements that are independently deliverable. A Component Assembly is two or more components associated together. Component Assemblies are utilized to perform operating system and/or applications tasks.
contain, contained, containing 683.2, 912.8, 912.35	Normal English: to have within or to hold. In the context of an element contained within a data structure (e.g., a secure container), the contained element may be either directly within the container or the container may hold a reference indicating where the element may be found.
control (n.) 193.1, 193.11, 193.15, 193.19, 891.1	Information and/or programming Governing operations on or use of Resources (e.g., content) including (a) permitted, required or prevented operations, (b) the nature or extent of such operations or (c) the consequences of such operations.
controlling, control (v.) 861.58, 193.1	Normal English: to exercise authoritative or dominating influence over; direct.
copied file 193.11	A Digital File that has been Copied and is usable.
copy, copied, copying 193.1, 193.11, 193.15, 193.19	Reproduce, reproduced, reproducing. The reproduction must be usable, may incorporate all of the original item or only some of it, and may involve some changes to the item as long as the essential nature of the content remains unchanged.
copy control 193.1	A Control used to determine whether a Digital File may be Copied and the Copied Digital File stored on a second device.
data item 891.1	A unit of digital information.
derive, derives 900.155	Normal English: obtain, receive or arrive at through a process of reasoning or deduction. In the context of computer operations, the "process of reasoning or deduction" constitutes operations carried out by the computer.
descriptive data structure 861.58	Machine-readable description of the layout and/or contents of a rights management data structure (e.g., a Secure Container).
designating 721.1	Normal English: indicating, specifying, pointing out or characterizing.
device class 721.1	A group of devices which share at least one attribute.
digital file 193.1, 193.11, 193.15, 193.19	A named collection of digital information.
digital signature, digitally signing 721.1	Digital signature: A digital value, verifiable with a Key, that can be used to determine the source and/or integrity of a signed item (e.g., a file, program, etc.). Digitally signing is the process of creating a digital signature.

3

Claim Term / Phrase	InterTrust Construction
entity's control 891.1	Entity's Control: Control belonging to or coming from an Entity. See list of Agreed Constructions for definition of Entity.
environment 912.35, 900.155, 891.1, 683.2, 721.34	Capabilities available to a program running on a computer or other device or to the user of a computer or other device. Depending on the context, the environment may be in a single device (e.g., a personal computer) or may be spread among multiple devices (e.g., a network).
executable programming, executable 912.8, 912.35, 721.34	A computer program that can be run, directly or through interpretation.
execution space, execution space identifier 912.8	Execution space: Resource which can be used for execution of a program or process. Execution space identifier: Information Identifying an Execution Space. See Authorization Information for definition of Information.
governed item 683.2	Governed Item: an item that is Governed. See list of Agreed Constructions for the definition of Governed.
halting 900.155	Normal English: suspending.
host processing environment 900.155	This term is explicitly defined in the claim and therefore needs no additional definition. It consists of those elements listed in the claim. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: a Protected Processing Environment incorporating software-based Security.
identifier, identify, identifying 193.11, 193.15, 912.8, 912.35, 861.58	Identifier: Information used to Identify something or someone (e.g., a password). Identify/identifying: Normal English: To establish/establishing the identity of or to ascertain/ascertaining the origin, nature, or definitive characteristics of; includes identifying as an individual or as a member of a group.
including 193.1 (at 320:63, and 321:3); 193.19 (at 324:15); 912.8 (at 327:36, 39, and 41); 912.35 (330:35 and 39); 861.58 (at 26:53 and 63); and 683.2 (at 63:60).	Normal English: Depending on the context, this means: part of or storing within, as opposed to Addressing.
information previously stored 900.155	Normal English: Information stored at an earlier time. See Authorization Information for the definition of Information.
integrity programming 900.155	This term is fully defined in the claim, which specifies the steps the integrity programming must perform. Integrity programming is programming that performs the recited steps. The term therefore needs no additional definition. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: programming that checks the integrity of a Host Processing Environment.

4

Claim Term / Phrase	InterTrust Construction
key 193.19	Information used to encrypt, decrypt, sign or verify other information.
load module 912.8, 721.1	An Executable unit of code designed to be loaded into memory and executed, plus associated data.
machine check programming 900.155	Programming that checks a host processing environment and derives information from an Aspect of the Host Processing Environment.
opening secure containers 683.2	Providing Access to the contents of a Secure Container (e.g., by decrypting the contents, if the contents are encrypted).
operating environment 891.1	Environment in which programs function.
organization, organization information, organize 861.58	In the context of organization of a Secure Container, these terms describe contents required or desired (including Information used to categorize these contents); or Information used to specify a particular location for content. See Authorization Information for the definition of Information.
portion 193.1, 193.11, 193.15, 193.19, 912.8, 912.35, 861.58	Normal English: a part of a whole. The presence of a "portion" does not exclude the presence of the whole (e.g., storage of an entire file necessarily includes storage of any portions into which that file may be subdivided).
prevents 721.34	Normal English: keeps from happening.
processing environment 912.35, 900.155, 721:34, 683.2	Processing: manipulating data. Processing Environment: An Environment used for Processing. A Processing Environment may be made up of one device or of more than one device linked together.
protected processing environment 721.34, 683.2	Processing Environment in which processing and/or data is at least in part protected from Tampering. The level of protection can vary, depending on the threat.
protecting 683.2	Normal English: keeping from being damaged, attacked, stolen or injured.
record (n.) 912.8, 912.35	Collection of related items of data treated as a unit.
required 912.8, 861.58	Normal English: a thing that is required is a thing that is obligatory or demanded.
resource processed 891.1	Resource: computer software, computer hardware, data, data structure or information. Resource processed: a Resource subject to being Processed, i.e., computer software, data, data structure or information. See Processing Environment for a definition of Processed.
rule 861.58, 683.2	See Control.

5

Claim Term / Phrase	InterTrust Construction
secure 193.1, 193.11, 193.15, 912.35, 861.58, 891.1, 683.2, 721.34	One or more mechanisms are employed to prevent, detect or discourage misuse of or interference with information or processes. Such mechanisms may include concealment, Tamper Resistance, Authentication and access control. Concealment means that it is difficult to read information (for example, programs may be encrypted). Tamper Resistance and Authentication are separately defined. Access control means that Access to information or processes is limited on the basis of authorization. Security is not absolute, but is designed to be sufficient for a particular purpose.
secure container 912.35, 861.58, 683.2	Container: Digital File Containing linked and/or embedded items. Secure Container: A Container that is Secure.
secure container governed item 683.2	Information and/or programming Contained in a Secure Container and Governed by an associated Secure Container Rule.
secure database 193.1, 193.11, 193.15	Database: an organized collection of information. Secure Database: Database that is Secure.
secure execution space 721.34	Execution Space that is Secure.
secure memory, memory 193.1, 193.11, 193.15	Memory: A medium in which data (including executable instructions) may be stored and from which it may be retrieved. "Memory" includes "virtual memory." Secure Memory: Memory in which Information is handled in a Secure manner. See Authorization Information for the definition of Information.
secure operating environment, said operating environment 891.1	An Operating Environment that is Secure.
securely applying 891.1	Requiring that one or more Controls be complied with before content may be used. The operation of requiring that the Control(s) be complied with must be carried out in a Secure manner.
securely assembling 912.8, 912.35	Associating two or more Components together to form a Component Assembly, in a Secure manner. See Component Assembly for the definition of Component.
securely processing 891.1	Processing occurring in a Secure manner. See Processing Environment for the definition of Processing.
securely receiving 891.1	Receiving has its normal English meaning: acquiring or getting. Securely Receiving means receipt occurring in a Secure manner.
security level, level of security 721.1; 721.34, 912.8	Information that can be used to determine how Secure something is (e.g., a device, Tamper Resistant Barrier or Execution Space).
tamper resistance 721.1, 721.34, 900.155	Making Tampering more difficult and/or allowing detection of Tampering.
tamper resistant barrier 721.34	Hardware and/or software that provides Tamper Resistance.

Claim Term / Phrase	InterTrust Construction
tamper resistant software 900.155	Software designed to make it more difficult to Tamper with the software and/or allow detection of tampering.
use 912.8, 912.35, 861.58, 193.19, 891.1, 683.2, 721.1	Normal English: to put into service or apply for a purpose, to employ.
user controls 683.2	Hardware feature of an apparatus allowing a user to operate the apparatus (e.g., a keyboard).
validity 912.8	A property of something (e.g., a Record) indicating that it is appropriate for use.
virtual distribution environment 900.155	This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: secure, distributed electronic transaction management and rights protection system for controlling the distribution and/or other usage of electronically provided and/or stored information.
'193:1	The claim contains no requirement of a VDE.
receiving a digital file including music	See Receiving a digital file (193.11). This phrase is interpreted the same, except that the file includes music.
a budget specifying the number of copies which can be made of said digital file	Normal English, incorporating the separately defined terms: a Budget stating the number of Copies that Can Be made of the Digital File referred to earlier in the claim.
controlling the copies made of said digital file	The nature of this operation is further defined in later claim elements. In context, the Copy Control determines the conditions under which a Digital File may be Copied and the Copied File stored on a second device.
determining whether said digital file may be copied and stored on a second device based on at least said copy control	Normal English, incorporating the separately defined terms: Using the Copy Control in deciding whether the Digital File referred to earlier in the claim may be Copied and the Copied Digital File stored on a second device.
if said copy control allows at least a portion of said digital file to be copied and stored on a second device	Normal English: a "yes" result is received in the step Determining whether said digital file may be copied and stored on a second device based on at least said copy control (193.1).
copying at least a portion of said digital file	Normal English, incorporating the separately defined terms: Copying at least a Portion of the Digital File referred to earlier in the claim.
transferring at least a portion of said digital file to a second device	Normal English, incorporating the separately defined terms: at least a Portion of the Copied Digital File is sent to a second device.
storing said digital file	Normal English: that which was transferred in the transferring step is stored.
'193:11	The claim contains no requirement of a VDE.
receiving a digital file	Normal English, incorporating the separately defined term: a Digital File is obtained. This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term:

Claim Term / Phrase	InterTrust Construction
	Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.
determining whether said digital file may be copied and stored on a second device based on said first control	Normal English, incorporating the separately defined terms: Using the Control to decide whether the Digital File may be Copied and the Copied Digital File stored on the second device.
identifying said second device	Normal English, incorporating the separately defined term: the second device is Identified.
whether said first control allows transfer of said copied file to said second device	Normal English, incorporating the separately defined terms: Using the first Control to decide if the Copied Digital File may be sent to the second device.
said determination based at least in part on the features present at the device	Normal English: the decision referred to earlier in the claim is based at least in part on characteristics of the second device.
if said first control allows at least a portion of said digital file to be copied and stored on a second device	See "If said copy control allows at least a portion of said digital file to be copied and stored on a second device" (193.1). The definitions are the same.
copying at least a portion of said digital file	See "Copying at least a portion of said digital file" (193.1). The definitions are the same.
transferring at least a portion of said digital file to a second device	See "Transferring at least a portion of said digital file to a second device" (193.1). The definitions are the same.
storing said digital file	See "Storing said digital file" (193.1). The definitions are the same.
'193:15	The claim contains no requirement of a VDE.
receiving a digital file	See "Receiving a digital file" (193.11). The definitions are the same.
an authentication step comprising:	Normal English, incorporating the separately defined term: a step involving Authentication.
accessing at least one identifier associated with a first device or with a user of said first device	Normal English, incorporating the separately defined terms: Accessing an Identifier Associated With a device or a user of the device.
determining whether said identifier is associated with a device and/or user authorized to store said digital file	Normal English, incorporating the separately defined terms: deciding whether the Identifier is Associated With a device or user with authority to store the Digital File.
storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized	Normal English, incorporating the separately defined terms: this step proceeds or does not proceed based on the preceding determining step. If this step proceeds, the Digital File is stored in a Secure Memory of the first device.
storing information associated with said digital file in a secure database stored on said first device, said information including	Normal English, incorporating the separately defined terms: storing a Control Associated With the Digital File in a Secure Database stored at the first device.

8

Claim Term / Phrase	InterTrust Construction
at least one control	
determining whether said digital file may be copied and stored on a second device based on said at least one control	See "Determining whether said digital file may be copied and stored on a second device based on at least said copy control" (193.1). The definitions are the same.
if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,	See "If said first control allows at least a portion of said digital file to be copied and stored on a second device" (193.11). The definitions are the same.
copying at least a portion of said digital file	See "Copying at least a portion of said digital file" (193.1). The definitions are the same.
transferring at least a portion of said digital file to a second device	See "Transferring at least a portion of said digital file to a second device" (193.1) The definitions are the same.
storing said digital file	See "Storing said digital file" (193.1) The definitions are the same.
'193:19	The claim contains no requirement of a VDE.
receiving a digital file at a first device	See "Receiving a digital file" (193.11). The definitions are the same.
establishing communication between said first device and a clearinghouse located at a location remote from said first device	Normal English, incorporating the separately defined term: sending information from the first device to the Clearinghouse and/or the first device receiving information from the Clearinghouse. This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term: Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.
using said authorization information to gain access to or make at least one use of said first digital file	Normal English, incorporating the separately defined terms: the Authorization Information is used in a process of Accessing or Using the Digital File.
receiving a first control from said clearinghouse at said first device	Normal English, incorporating the separately defined terms: the first device acquires or gets a Control from the Clearinghouse. This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term: Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.
storing said first digital file in a memory of said first device	Normal English, incorporating the separately defined terms: the Digital File is stored at the first device.

9

Claim Term / Phrase	InterTrust Construction
using said first control to determine whether said first digital file may be copied and stored on a second device	See "Determining whether said digital file may be copied and stored on a second device based on at least said copy control" (193.1). The definitions are the same.
if said first control allows at least a portion of said first digital file to be copied and stored on a second device	See "If said first control allows at least a portion of said digital file to be copied and stored on a second device" (193.11). The definitions are the same.
copying at least a portion of said first digital file	See "Copying at least a portion of said digital file" (193.1). The definitions are the same.
transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output	See "Transferring at least a portion of said digital file to a second device" (193.1). The definitions are the same, except that the second device has an audio or video output or both (e.g., a speaker, a screen, etc.).
storing said first digital file portion	Normal English, incorporating the separately defined terms: the Digital File Portion is stored.
'683:2	The claim contains no requirement of a VDE.
the first secure container having been received from a second apparatus	Normal English, incorporating the separately defined term: the Secure Container was acquired from a second apparatus. The second apparatus is different from the first apparatus.
an aspect of access to or use of	Normal English, incorporating the separately defined terms: Aspect and Access to or Use of. Those terms fully define the phrase, so that no other definition is possible.
the first secure container rule having been received from a third apparatus different from said second apparatus	Normal English, incorporating the separately defined terms: this term requires that the first Secure Container Rule was acquired from a third apparatus. The third apparatus is different from the second apparatus or the first apparatus.
hardware or software used for receiving and opening secure containers	Normal English, incorporating the separately defined terms: computer hardware or programming that acquires Secure Containers and Opens the Secure Containers (see Opening Secure Containers). This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies structures corresponding to this term: Structures corresponding to this element include Processor(s) 4126 and/or software running on Processors 4126 (including Protected Processing Environment 650) and Communications Device 666.
said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers	Each Secure Container referred to in the phrase "hardware or software used for receiving and opening secure containers" must have the capacity to Contain a Governed Item, and must have Associated With it a Secure Container Rule.
protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus	Normal English, incorporating the separately defined terms: a Protected Processing Environment contains Information. The Protected Processing Environment protects the contained Information from Tampering by a user. The protection may be partial rather than complete. See Authorization Information for the definition of Information.

Claim Term / Phrase	InterTrust Construction
hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container	Normal English, incorporating the separately defined terms: computer hardware or programming that uses the first Secure Container Rule and a second Secure Container Rule. These rules are Applied in Combination to Govern a Governed Item contained in a Secure Container.

This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies structures corresponding to this term:

Structures corresponding to this element include Processor(s) 4126 and/or software running on Processors 4126 (including Protected Processing Environment 650). |
| hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses. | Normal English, incorporating the separately defined terms: computer hardware or programming that sends Secure Containers to other apparatuses (e.g., other computers) or acquires Secure Containers from other apparatuses.

This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies structures corresponding to this term:

Structures corresponding to this element include Processor(s) 4126 and/or software running on Processors 4126 (including Protected Processing Environment 650) and Communications Device 666. |
'721:1	The claim contains no requirement of a VDE.
digitally signing a first load module with a first digital signature designating the first load module for use by a first device class	Normal English, incorporating the separately defined terms: generating a Digital Signature for the first Load Module, the Digital Signature Designating that the first Load Module is for use by a first Device Class.
digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class	Normal English, incorporating the separately defined terms: generating a Digital Signature for the second Load Module, the Digital Signature Designating that the second Load Module is for use by a second Device Class. This element further requires that the second Device Class have a different Tamper Resistance or Security Level than the first Device Class.
distributing the first load module for use by at least one device in the first device class	Normal English, incorporating the separately defined terms: distributing the first Load Module so that it can be used by a device in the first Device Class.
distributing the second load module for use by at least one device in the second device class	Normal English, incorporating the separately defined terms: distributing the second Load Module so that it can be used by a device in the second Device Class.
'721:34	The claim contains no requirement of a VDE.
arrangement within the first tamper resistant barrier	Normal English, incorporating the separately defined terms: an Arrangement protected by the first Tamper Resistant Barrier, the Arrangement operating as described in the claim.

11

Claim Term / Phrase	InterTrust Construction
prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level	Normal English, incorporating the separately defined terms: stops the first Secure Execution Space from executing (e.g. running a program) an Executable accessed by a second Secure Execution space. The first and second Secure Execution Spaces have Tamper Resistant Barriers that have different Security Levels.
'861:58	The claim contains no requirement of a VDE.
creating a first secure container	This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: Normal English, incorporating the separately defined terms: producing a Secure Container.
including or addressing . . . organization information . . . desired organization of a content section. . . and metadata information at least in part specifying at least one step required or desired in creation of said first secure container	This is not a claim term, but is instead a series of fragments. Interpretation of this phrase is therefore impossible, since the phrase does not appear in the claim. Without waiving its position that these claim fragments should not be interpreted, InterTrust would be willing to agree to the following: 1. The same single Descriptive Data Structure must either Contain within its confines or Address both Organization Information and Metadata information.
at least in part determine specific information required to be included in said first secure container contents	Normal English, incorporating the separately defined terms: at least partially Identify specific Information that must be included in the first Secure Container. See Authorization Information for the definition of Information.
rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents	Normal English, incorporating the separately defined terms: a Rule that Governs at least some of the contents of the Secure Container.
'891:1	The claim contains no requirement of a VDE.
resource processed in a secure operating environment at a first appliance	This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: Normal English, incorporating the separately defined terms: a Resource Processed in a Secure Operating Environment, the Secure Operating Environment being present at an appliance (e.g., a computer).
securely receiving a first entity's control at said first appliance	Normal English, incorporating the separately defined terms: an Entity's Control is Securely Received at the first appliance. This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term: Claim elements specifying the act of receiving a file, or the act of establishing

Claim Term / Phrase	InterTrust Construction
	communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc. Claim elements specifying the act of "securely receiving" map onto embodiments of "receiving" (see above) in which the received element (e.g., a control) is received in a manner providing security. The specification describes a number of security-related mechanisms for use in communications, including encryption, authentication and tamper-resistance. Such mechanisms constitute alternate embodiments.
securely receiving a second entity's control at said first appliance	See Securely receiving a first entity's control at said first appliance. The definitions are the same, except that the second entity and the first entity are different.
securely processing a data item at said first appliance, using at least one resource	Normal English, incorporating the separately defined terms: a Resource is used in Securely Processing a Data Item, the processing occurring at the first appliance.
securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item	Normal English, incorporating the separately defined terms: the first Entity's Control and the second Entity's Control are Securely Applied to Govern Use of the Data Item, the act of Securely Applying involving use of the Resource.
'900:155	See definition of Virtual Distribution Environment, above.
first host processing environment comprising	A Host Processing Environment including (but not limited to), the listed elements.
designed to be loaded into said main memory and executed by said central processing unit	Normal English, incorporating the separately defined term: software designed to be loaded into the Memory of a computer and executed by the computer's processor.
said tamper resistant software comprising: . . . one or more storage locations storing said information	This is not a claim term, but is instead two sentence fragments. Interpretation of this phrase is therefore impossible, since the phrase does not appear in the claim.
derives information from one or more aspects of said host processing environment,	Normal English, incorporating the separately defined terms: Derives (including creates) Information based on at least one Aspect of the previously referred to Host Processing Environment. See Authorization Information for the definition of Information.
one or more storage locations storing said information	Normal English, incorporating the separately defined terms: Information relating to one or more Aspects of the Host Processing Environment is stored in one or more locations. See Authorization Information for the definition of Information.
information previously stored in said one or more storage locations	See Information Previously Stored. The definitions are the same.
generates an indication based on the result of said comparison	Producing an indication based on the result of the "compares" step. The "indication" need not be displayed to a user.
programming which takes one or more actions based on the state of said indication	Normal English: software that takes an action if the indication has one state, but does not take that action if the indication does not have that state.
at least temporarily halting further processing	Normal English, incorporating the separately defined terms: Halting Processing, the Halt being temporary or permanent. See Securely Processing for the definition of Processing.

Claim Term / Phrase	InterTrust Construction
	Processing.
'912:8	The claim contains no requirement of a VDE.
identifying at least one aspect of an execution space required for use and/or execution of the load module	Identifying at least one aspect of an execution space: Normal English, incorporating the separately defined terms: Identifying an Aspect (e.g. Security Level) of an Execution Space Required for use and/or execution of the load module: Normal English, incorporating the separately defined terms: the Identified Aspect is needed in order for the Load Module to execute or otherwise be used.
said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security	Normal English, incorporating the separately defined terms: the Execution Space Identifier makes it possible to distinguish higher Security Level Execution Spaces from lower Security level Execution Spaces.
checking said record for validity prior to performing said executing step	Normal English, incorporating the separately defined terms: determining whether the Record has Validity, the determination occurring before the execution step.
'912:35	The claim contains no requirement of a VDE.
received in a secure container	Normal English, incorporating the separately defined terms: the Record is Contained in a Secure Container when acquired.
said component assembly allowing access to or use of specified information	Normal English, incorporating the separately defined terms: the Component Assembly allows Access to specified Information. See Authorization Information for the definition of Information.
said first component assembly specified by said first record	This term is a label referring back to the first component assembly identified earlier in the claim. It has no other meaning.

Exhibit C

EXHIBIT C

PLR 4-3(b) – Identification of Supporting Evidence

The following represents InterTrust's list of all evidence relevant to construction of the disputed terms and phrases. InterTrust expects to identify those passages of greatest significance in connection with InterTrust's claim construction briefing. In addition to the evidence listed in the table below, InterTrust intends to rely on the testimony of Dr. Reiter, as described in more detail in Exh. F.

Notes:

      1. InterTrust reserves the right to supplement this list as needed to respond to changed constructions proffered by Microsoft immediately before or after the submission of the Joint Claim Construction Statement, or to respond to evidence or arguments proffered by Microsoft.

      2. In the following list, certain terms and phrases include other, separately defined terms. In such cases, the evidence supporting the separately defined term is also relevant to construction of the larger term.

      3. The InterTrust patents include overlapping specifications, in which the same text may be found in two or more specifications. In such cases, InterTrust has cited only one of the specifications. InterTrust reserves the right to substitute citations for the same text in other specifications.

      4. Citations of specification text also include a citation of any Figures discussed in that text.

      5. Each claim term is followed by a list of all patent claims in which the term appears (e.g., "193.15" means claim 15 from the '193 patent).

Key to abbreviations:
    USP = United States Patent
    '193 patent = USP 6,253,193
    '683 patent = USP 6,185,683
    '721 patent = USP 6,157,721
    '891 patent = USP 5,982,891
    '861 patent = USP 5,920,861
    '912 patent = USP 5,917,912
    '900 patent = USP 5,892,900

Claim Term / Phrase	InterTrust Evidence
access, accessed, access to, accessing 193.15, 193.19, 912.8, 912.35, 861.58, 683.2, 721.34	**Patent Specifications** '193 patent at 51:32-33, 61 '193 patent at 59:53-55 '193 patent at 62:54-57 '193 patent at 64:6-7 '193 patent at 65:14-19 '193 patent at 71:49-51 '193 patent at 72:1-3 '193 patent at 120:59-66 '193 patent at 128:42-45 '193 patent at 136:58-60 '193 patent at 137:63-66 '193 patent at 139:41-55 '193 patent at 159:24-26 '193 patent at 159:64-160:8 '193 patent at 163:36-63 '193 patent at 170:17-19

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 173:9-16 '193 patent at 178:57-63 '193 patent at 183:24-26 '193 patent at 183:55-57 '193 patent at 188:65-66 '193 patent at 192:2-57 '193 patent at 217:27-42 '193 patent at 274:58-61 '193 patent at 298:67-299:5 '683 patent at 10:66-11:3 '683 patent at 12:52-53 '683 patent at 13:15 '683 patent at 15:67-16:4 '683 patent at 19:6-14 '683 patent at 42:34-37 '683 patent at 56:21-25 '683 patent at 57:63-65 '861 patent at 12:35-39 '861 patent at 13:6-17 '861 patent at 15:35-48 '861 patent at 17:22-25 '721 patent at 2:47-53 '721 patent at 2:62-63 '721 patent at 4:5-15 **Extrinsic Sources** Personal Computer Dictionary (1995), p. 11. Wyatt, Computer Professional's Dictionary (Osborne McGraw-Hill, 1990), p. 7. Webster's New World Dictionary of Computer Terms, 6th ed. (1997), p. 12. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** The New IEEE Standard Dictionary of Electrical and Electronic Terms (IEEE, 1993), p. 6. Cooper, Computer & Communications Security: Strategies for the 1990s, p. 365. National Information System Security (INFOSEC) Glossary, NSTISSI No. 4009 (2000), p. 1. Glossary of Telecommunications Terms (National Communications Systems, 1996), p. A-3. Webster's New World Dictionary of Computer Terms, 4th ed. (1992), p. 2. Encyclopedia of Computer Science and Engineering, 2nd ed. (Van Nostrand Reinhold, 1983), p. 494.
addressing 861.58	**Patent Specifications** '861 patent at 5:57-6:7 '861 patent at 10:53-59 '861 patent at 14:14-29 '861 patent at 15:21-31

2

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 86:51-56 '193 patent at 92:18-23 '193 patent at 109:2-5 '193 patent at 214:15-18 '193 patent at 289:14-22 **Extrinsic Sources** Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 17. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** The New IEEE Standard Dictionary of Electrical and Electronic Terms (1993), pp. 16-17. Glossary of Telecommunications Terms (National Communications Systems, 1996), p. A-7.
allowing, allows 912.35, 193.1, 193.11, 193.15, 193.19	**Patent Specifications** '193 patent at 11:19-23 '193 patent at 15:14-17 '193 patent at 16:49-51 '193 patent at 34:13-19 '193 patent at 75:1-5 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 50. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Webster's College Dictionary of Random House (1991), p. 38. Funk & Wagnalls Standard College Dictionary (1973-74), p. 39.
arrangement 721.34	**Patent Specifications** '721 patent at 3:10-15 '721 patent at 4:56-60 '721 patent at 16:52-64 '721 patent at 19:24-32 '193 patent at 1:27-36 '193 patent at 8:21-27 '193 patent at 10:49-53 '193 patent at 11:38-45 '193 patent at 11:49-53 '193 patent at 12:51-61 '193 patent at 13:1-4 '193 patent at 14:60-66 '193 patent at 19:5-9 '193 patent at 20:51-67 '193 patent at 41:31-33 '193 patent at 45:52-59 '193 patent at 48:33-36 '193 patent at 48:66-49:3 '193 patent at 225:39-46 '193 patent at 226:43-53 '193 patent at 227:25-28 '193 patent at 230:45-50 '193 patent at 236:25-29

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 301:58-59 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 102. **File Histories** '721 File History, original claims 15-18 and 36-39
aspect 900.155, 912.8, 861.58, 683.2	**Patent Specifications** '900 patent at 74:49-55 '900 patent at 74:12-17 '900 patent at 74:29-33 '900 patent at 77:15-19 '900 patent at 236:3-7 '193 patent at 83:30-32 '193 patent at 95:27-30 '193 patent at 103:14-20 '193 patent at 121:35-37 '193 patent at 125:39-41 '193 patent at 260:42-47 '193 patent at 340:40-43 '861 patent at 6:24-29 '861 patent at 17:3-6 **File Histories** '900 File History, original claims 5-6. App. No. 09/342,899, 6/12/00 Office Action, p. 5 (citing USP 5,748,960 at 21:7-15).
associated with 912.8, 193.1, 193.11, 193.15, 683.2	**Patent Specifications** '193 patent at 5:19-21 '193 patent at 12:40-43 '193 patent at 13:54-63 '193 patent at 15:51-55 '193 patent at 17:52-56 '193 patent at 18:36-42 '193 patent at 20:8-26 '193 patent at 22:20-25 '193 patent at 32:49-51 '193 patent at 33:26-30 '193 patent at 55:5-11 '193 patent at 55:39-51 '193 patent at 57:17-40 '193 patent at 59:6-18 '193 patent at 65:66-66:5 '193 patent at 103:54-104:28 '193 patent at 149:46-54 '193 patent at 153:32-154:49 '193 patent at 188:8-11 '193 patent at 194:47-51 '193 patent at 195:10-24 '193 patent at 210:56-211:9 '193 patent at 241:17-26 '193 patent at 245:9-13

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 268:66-269:11 '193 patent at 269:23-34 '193 patent at 292:63-67 '193 patent at 297:61-298:2 '193 patent at 299:46-49 '193 patent at 300:44-51 '193 patent at 308:48-56 '683 patent at 8:34-37 '683 patent at 9:56-58 '683 patent at 10:1-4 '683 patent at 24:5-13 '683 patent at 26:12-16 '683 patent at 27:24-28 '683 patent at 30:44-56 '683 patent at 37:14-19 '683 patent at 40:10-15 '683 patent at 41:58-61
authentication 193.15	**Patent Specifications** '193 patent at 13:33-37 '193 patent at 64:29-37 '193 patent at 67:58-60 '193 patent at 115:17-21 '193 patent at 123:21-62 '193 patent at 160:24-26 '193 patent at 203:58-61 '193 patent at 204:2-11 '193 patent at 204:27-34 '193 patent at 213:1-15 '193 patent at 218:38-220:19 '193 patent at 230:22-27 '193 patent at 232:47-53 '193 patent at 236:21-25 '193 patent at 290:47-62 '193 patent at 319:27-29 '683 patent at 7:42-45 '683 patent at 8:15-27 '683 patent at 10:1-4 '683 patent at 18:65-19:26 '683 patent at 21:36-52 '683 patent at 30:65-31:63 '683 patent at 34:54-57 '683 patent at 41:18-21 '683 patent at 48:32-36 '683 patent at 49:1-17 **File Histories** '683 File History, 11/12/99 Office Action, p. 7 (citing USP 5,412,717 at 6:19-48). **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Tanenbaum, Modern Operating Systems (Prentice Hall, 1992), p. 189.
authorization information, authorized, not authorized	**Patent Specifications** '193 patent at 3:3-9 '193 patent at 167:8-11

Claim Term / Phrase	InterTrust Evidence
193.15, 193.19	'193 patent at 167:55-59 '193 patent at 211:39-212:7 '193 patent at 214:42-48 '193 patent at 215:59-216:5 '193 patent at 220:47-52 '193 patent at 223:57-60 '193 patent at 254:40-44 **File Histories** USP 5,910,987 File History, 9/23/98 Office Action, p. 4. **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 120. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Cooper, Computer & Communications Security: Strategies for the 1990s, p. 367. Laplante, Dictionary of Computer Science, Engineering and Technology (2001), p. 29. Microsoft Computer Dictionary, 2nd ed. (Microsoft Press, 1994), p. 32. Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 36.
budget control; budget 193.1	**Patent Specifications** '193 patent at 22:47-52 '193 patent at 50:18 '193 patent at 51:44-45 '193 patent at 57:51-54 '193 patent at 58:26-34 '193 patent at 58:38-59:37 '193 patent at 130:58-131:52 '193 patent at 132:7-26 '193 patent at 132:55-65 '193 patent at 133:12-13 '193 patent at 133:45-59 '193 patent at 142:41-61 '193 patent at 143:10-28 '193 patent at 143:38-144:31 '193 patent at 150:63-66 '193 patent at 152:44-47 '193 patent at 172:14-48 '193 patent at 172:61-174:33 '193 patent at 173:21-177:53 '193 patent at 182:7-14 '193 patent at 182:22-30 '193 patent at 184:67-185:1 '193 patent at 220:20-40 **File Histories** App. No. 09/328,668, 9/1/00 Office Action, p. 4. USP 5,910,987 File History, 9/23/98 Office Action, p. 5. **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 249
can be	**Extrinsic Sources**

Claim Term / Phrase	InterTrust Evidence
193.1	The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), pp. 159, 277.
capacity 683.2	**Patent Specifications** '193 patent at 127:35-62 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 283. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Webster's College Dictionary of Random House (1991), p. 201. Random House Dictionary of the English Language: College Edition (1968), p. 200. Encyclopedia of Computer Science and Engineering, 2nd ed. (Van Nostrand Reinhold, 1983), pp. 208, 1519
clearinghouse 193.19	**Patent Specifications** '193 patent at 3:32-33 '193 patent at 13:17-23 '193 patent at 25:22-24 '193 patent at 36:15-48 '193 patent at 41:8-9 '193 patent at 47:37-42 '193 patent at 50:8-9 '193 patent at 55:57-66 '193 patent at 56:16-24 '193 patent at 132:35-37 '193 patent at 161:66-162:65 '193 patent at 253:65-254:1 '193 patent at 255:33-51 '193 patent at 267:40-42 '193 patent at 268:29-31 '193 patent at 269:59-65 '193 patent at 270:42-58 '193 patent at 271:44-49 '193 patent at 280:18-26 '193 patent at 284:50-59 **File Histories** USP 6,427,140 File History, 3/30/01 Office Action, p. 3. USP 6,112,181 File History, 12/31/98 Office Action, p. 30. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Encyclopedia of Computer Science and Engineering, 2nd ed. (Van Nostrand Reinhold, 1983), p. 600.
compares, comparison 900.155	**Patent Specifications** '900 patent at 195:9-12 '900 patent at 280:63-65 '900 patent at 322:15-20 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 384. **Citations from Sources Designated by Microsoft under PLR 4-2(b)**

Claim Term / Phrase	InterTrust Evidence
	The New IEEE Standard Dictionary of Electrical and Electronic Terms (IEEE, 1993), p. 221. Illustrated Dictionary of Computing, 2nd ed. (Prentice Hall, 1992), p. 110. The American Heritage Dictionary of the English Language (1969), p. 271. Webster's College Dictionary of Random House (1991), p. 276. Funk & Wagnalls Standard College Dictionary (1973-74), p. 275. Random House Dictionary of the English Language: College Edition (1968), p. 273. Webster's Ninth New Collegiate Dictionary (Merriam-Webster, 1987), pp. 276-277. IBM Dictionary of Computing (McGraw Hill, 1994), pp. 124-125.
component assembly 912.8, 912.35	**Patent Specifications** '193 patent at 25:54-26:9 '193 patent at 50:35-36 '193 patent at 83:12-88:21 '193 patent at 112:46-113:62 '193 patent at 115:43-116:51 '193 patent at 133:43-45 '193 patent at 138:31-37 '193 patent at 159:61-160:8 '193 patent at 169:62-170:4 '193 patent at 171:39-42 '193 patent at 247:58-64 '193 patent at 250:21-34 '193 patent at 260:36-47 **File Histories** '912 File History, 9/22/98 Office Action, pp. 2-3 (citing USP 5,748,960); see also USP 5,748,960 at 1:33-67 and 16:32-41. '912 File History, 6/24/98 Amendment, pp. 73-75. '912 File History, 12/24/97 Office Action, pp. 2-3 (citing USP 5,629,980; USP 5,499,298; and USP 5,457,746); see also USP 5,629,980 at 9:6-11:29; USP 5,499,298 at 6:46-8:23; and USP 5,457,746 at 10:8-67. App. No. 09/342,899 File History, 12/12/00 Amendment, p. 7. App. No. 09/342,899 File History, 12/13/01 Response, p. 3.
contain, contained, containing 683.2, 912.8, 912.35	**Patent Specifications** '193 patent at 19:15-21 '193 patent at 58:48-58 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 406. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Webster's College Dictionary of Random House (1991), p. 293.

Claim Term / Phrase	InterTrust Evidence
	Random House Dictionary of the English Language: College Edition (1968), p. 289.
	Que's Computer Programmer's Dictionary (1993), p. 93.
control (n.) 193.1, 193.11, 193.15, 193.19, 891.1	**Patent Specifications** '193 patent at 5:19-24 '193 patent at 6:33-45 '193 patent at 7:13-19 '193 patent at 10:66-11:18 '193 patent at 12:12-14 '193 patent at 13:54-60 '193 patent at 15:3-7 '193 patent at 15:18-21 '193 patent at 15:33-38 '193 patent at 15:46-50 '193 patent at 17:15-21 '193 patent at 17:46-67 '193 patent at 18:29-42 '193 patent at 19:13-32 '193 patent at 22:47-58 '193 patent at 25:48-52 '193 patent at 25:52-26:12 '193 patent at 28:19-44 '193 patent at 29:21-28 '193 patent at 30:62-65 '193 patent at 32:30-34 '193 patent at 33:11-19 '193 patent at 33:63-34:3 '193 patent at 34:30-37 '193 patent at 42:21-38 '193 patent at 42:39-43:1 '193 patent at 43:25-44:2 '193 patent at 44:34-52 '193 patent at 45:11-15 '193 patent at 45:33-36 '193 patent at 48:29-35 '193 patent at 49:11-12 '193 patent at 49:50-55 '193 patent at 53:53-59 '193 patent at 56:26-32 '193 patent at 57:27-36 '193 patent at 57:51-55 '193 patent at 58:27-34 '193 patent at 59:1-25 '193 patent at 71:20-25 '193 patent at 77:32-34 '193 patent at 77:45-63 '193 patent at 77:64-78:3 '193 patent at 78:6-9 '193 patent at 110:54-55 '193 patent at 121:15-32 '193 patent at 127:6-26 '193 patent at 128:25-33 '193 patent at 129:52-60 '193 patent at 129:64-67 '193 patent at 130:26-29 '193 patent at 130:41

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 131:33-50
	'193 patent at 131:59-132:18
	'193 patent at 135:49-58
	'193 patent at 137:4-7
	'193 patent at 148:59-149:7
	'193 patent at 149:13-153:31
	'193 patent at 169:5-13
	'193 patent at 174:15-177:53
	'193 patent at 182:43-44
	'193 patent at 217:40-42
	'193 patent at 242:7-53
	'193 patent at 243:28-37
	'193 patent at 245:9-14
	'193 patent at 247:30-51
	'193 patent at 247:61-248:8
	'193 patent at 258:53-55
	'193 patent at 264:16-19
	'193 patent at 264:40-49
	'193 patent at 268:62-64
	'193 patent at 271:58-61
	'193 patent at 276:10-17
	'193 patent at 280:49-58
	'193 patent at 284:22-26
	'193 patent at 293:24-29
	'193 patent at 293:64-294:1
	'193 patent at 297:61-298:2
	'193 patent at 298:54-62
	'193 patent at 301:66-302:2
	'193 patent at 314:58-64
	'193 patent at 315:52-60
	File Histories
	'193 File History, 12/20/96 Office Action, pp. 2-3.
	'193 File History, 6/20/97 Response, pp. 23-25.
	'193 File History, 6/7/00 Office Action, pp. 2-4 (citing USP 4,595,950); see also USP 4,595,950 at 4:4-18; 4:28-33; 4:38-54; 4:64-5:20; 5:35-58; 6:38-65; 7:5-41; 8:48-57; 9:1-39; 9:54-66; and 12:29-13:33.
	'900 File History, 8/27/98 Office Action, pp. 3-4 (citing USP 5,048,085 at 2:41-46).
	'891 File History, 12/20/96 Office Action, pp. 2-3
	USP 5,915,019 File History, 7/28/97 Office Action, pp. 2-3 (citing USPs 5,638,443; 5,563,946; USP 5,509,070; and 5,504,818); see also USP 5,638,443 at 10:61-11:67; USP 5,563,946 at 8:27-58 and 9:25-39; USP 5,509,070 at 7:10-8:9; and USP 5,504,818 at 6:33-67.
	USP 5,915,019 File History, 4/15/98 Office Action, pp. 3-4 (citing USP 5,311,591); see also 5,311,591 at 2:14-46; 11:4-10; and 12:7-20.
	USP 6,389,402 File History, 3/15/00 Office Action, p. 2.
	09/328,668 File History, 9/1/00 Office Action, p. 4.
	USP 5,910,987 File History, 9/23/98 Office Action, p.4 (citing USP 5,412,717 at 9:33-57); see also USP 5,412,717 at 2:24-26; 5:3-7; and Figs. 2 and 3(c).

Claim Term / Phrase	InterTrust Evidence
	USP 6,363,488 File History, 12/19/00 Office Action, p. 2-4 (citing USP 4,658,093); see also USP 4,658,093 at 4:48-63, and Abstract). USP 6,237,786 File History, 7/17/00 Office Action, pp. 2-3 (citing USP 4,827,508); see also USP 4,827,508 at 8:61-9:2; 9:32-36; 19:8-26; and 21:39-55). USP 6,112,181 File History, 12/31/98 Office Action, p. 14 (citing USP 5,740,549 at 16:45-54). USP 5,949,876 File History, 7/18/97 Office Action, pp. 2-3 (citing USP 5,504,837 at 7:48-8:44; USP 5,508,913 at 3:56-4:11; and USP 5,260,999 at 42:63-43:20 and 45:18-30).
controlling, control (v.) 861.58, 193.1	**Patent Specifications** '193 patent at 15:46-50 '193 patent at 33:26-30 '193 patent at 62:58-60 '193 patent at 63:39-44 '193 patent at 64:55-58 '193 patent at 65:35-38 '193 patent at 68:46-49 '193 patent at 68:51-53 '193 patent at 76:37-41 '193 patent at 77:48-57 '193 patent at 128:41-46 '193 patent at 139:60-140:1 '193 patent at 159:23-26 '193 patent at 172:51-55 '193 patent at 174:15-29 '193 patent at 241:17-26 '193 patent at 268:29-31 '193 patent at 273:42-46 '193 patent at 288:11-12 '193 patent at 296:13-14 '683 patent at 24:33-39 '683 patent at 27:22-24 **File Histories** '683 File History, 11/12/99 Office Action, p. 13. USP 6,389,402 File History, 12/6/00 Office Action, p. 3. USP 6,363,488 File History, 12/19/00 Office Action, p. 2. USP 6,427,170 File History, 3/3/01 Office Action, p. 4. **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), pp. 410, 784. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Laplante, Dictionary of Computer Science, Engineering and Technology (2001), p. 104. Webster's College Dictionary of Random House (1991), p. 297. Funk & Wagnalls Standard College Dictionary (1973-74), p. 295.

Claim Term / Phrase	InterTrust Evidence
	Random House Dictionary of the English Language: College Edition (1968), p. 293. Webster's Ninth New Collegiate Dictionary (Merriam-Webster, 1987), p. 285.
copied file 193.11	**Patent Specifications** '193 patent at 325:32-40 See Digital File; Copy; Copy Control
copy, copied, copying 193.1, 193.11, 193.15, 193.19	**Patent Specifications** '193 patent at 20:36-43 '193 patent at 23:10-15 '193 patent at 25:18-24 '193 patent at 26:59-67 '193 patent at 28:19-23 '193 patent at 37:27-36 '193 patent at 37:59-64 '193 patent at 48:29-35 '193 patent at 53:60-62 '193 patent at 57:67-58:3 '193 patent at 80:40-48 '193 patent at 109:15-22 '193 patent at 131:10-17 '193 patent at 131:65-132:1 '193 patent at 143:14-18 '193 patent at 159:24-26 '193 patent at 167:63-67 '193 patent at 194:14-19 '193 patent at 226:11-16 '193 patent at 264:29-49 '193 patent at 279:3-9 '193 patent at 288:46-52 '193 patent at 319:12-15 '193 patent at 323:50-324:7 **Extrinsic Sources** Personal Computer Dictionary (1995), p. 47. The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 416. Webster's New World Dictionary of Computer Terms, 6th Edition (1997), p. 118. Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 120. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Dictionary of Scientific and Technical Terms, 5th ed. (McGraw-Hill, 1994), p. 461. See Copied File
copy control 193.1	**Patent Specifications** '193 patent at 38:4-9 '193 patent at 48:12-35 '193 patent at 65:24-38 '193 patent at 68:51-61

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 72:1-9 '193 patent at 133:39-50 '193 patent at 162:10-15 '193 patent at 167:41-43 '193 patent at 220:28-40 '193 patent at 226:11-16 '193 patent at 237:34-47 '193 patent at 252:51-58 '193 patent at 264:28-57 '193 patent at 278:9-25 '193 patent at 316:16-317:19 '193 patent at 322:46-323:7 '193 patent at 325:32-40
data item 891.1	**Patent Specifications** '193 patent at 9:27-31 '193 patent at 58:48-57 '193 patent at 67:56-57 '193 patent at 126:8-52 '193 patent at 312:63-66 **Extrinsic Sources** Wyatt, Computer Professional's Dictionary (Osborne McGraw-Hill, 1990), p. 101. Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 131. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Microsoft Computer Dictionary, 2nd ed. (Microsoft Press, 1994), pp. 107-108. Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 130. McNulty, Security on the Internet, Statement Before the Subcommittee on Science, Committee on Science, Space, and Technology, U S House of Representatives (Mar. 22, 1994), p. 9 ("Data Integrity - Verification that the contents of a data item (e.g., message, file, program) have not been accidentally or intentionally changed in an unauthorized manner").
derive, derives 900.155	**Patent Specifications** '900 patent at 73:38-42 '900 patent at 74:36-42 '900 patent at 75:30-36 '900 patent at 75:41-49 '900 patent at 245:25-39 '900 patent at 247:4-12 '900 patent at 247:20-26 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 504. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Webster's College Dictionary of Random House (1991), p. 365. Funk & Wagnalls Standard College Dictionary (1973-74), p. 360. Random House Dictionary of the English Language: College Edition (1968), p. 358.

Claim Term / Phrase	InterTrust Evidence
	See "Derives information from one or more aspects of said host processing environment" (900.155).
descriptive data structure 861.58	**Patent Specifications** '861 patent at 5:26-37 '861 patent at 5:57-6:7 '861 patent at 6:8-10 '861 patent at 6:19-23 '861 patent at 6:24-31 '861 patent at 6:38-47 '861 patent at 7:42-9:63 '861 patent at 10:49-61 '861 patent at 11:15-24 '861 patent at 11:25-47 '861 patent at 11:58-12:5 '861 patent at 13:41-14:12 '861 patent at 14:13-29 '861 patent at 15:21-34 '861 patent at 16:11-31 '861 patent at 17:13-31 '861 patent at 17:35-53 '861 patent at 17:61-18:5 **File Histories** '861 File History, 6/25/98 Office Action, p. 3 (citing USP 5,537,526); see also USP 5,537,526 at 7:9-67; 10:12-39 and 16:10-20. USP 6,138,119 File History, 4/26/00 Office Action, p. 9.
designating 721.1	**Patent Specifications** '721 patent at 7:66-8:2 '193 patent at 103:11-20 '193 patent at 150:30-33 '193 patent at 154:64-155:6 '193 patent at 246:64-66 '193 patent at 277:56-278:16 '193 patent at 280:1-4 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 506.
device class 721.1	**File Histories** '721 File History, 4/13/99 Amendment, p. 14. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** The American Heritage Dictionary of the English Language (1969), p. 248. Webster's College Dictionary of Random House (1991), pp. 250-251, 370. Funk & Wagnalls Standard College Dictionary, (1973-74), p. 251.
digital file	**Patent Specifications** '193 patent at 45:66-46:3

Claim Term / Phrase	InterTrust Evidence
193.1, 193.11, 193.15, 193.19	'193 patent at 123:66-67 '193 patent at 165:25-30 '193 patent at 167:33-35 '193 patent at 258:30-43 **Extrinsic Sources** Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 194. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Encyclopedia of Computer Science and Engineering, 2nd ed. (Van Nostrand Reinhold, 1983), p.494. Hutt et al., Computer Security Handbook, 2d ed (Macmillan, 1988), p. 218.
digital signature, digitally signing 721.1	**Patent Specifications** '721 patent at 4:32-35 '721 patent at 4:64-5:5 '721 patent at 6:5-15 '721 patent at 6:42-52 '721 patent at 7:11-18 '721 patent at 7:47-57 '721 patent at 10:56-59 '721 patent at 10:60-64 '721 patent at 12:67-13:3 '721 patent at 14:61-15:16 '721 patent at 15:31-34 **Extrinsic Sources** Dictionary of Information Technology, 3d ed. (Van Nostrand Reinhold, 1989) **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Russell et al., Computer Security Basics (O'Reilly & Associates, 1991), p. 410. Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 145. Garfinkel et al., Practical Unix Security (O'Reilly & Associates, 1991), p. 122. Neumann, Computer Related Risks (ACM Press, 1995), p. 345.
entity's control 891.1	**Patent Specifications** '193 patent at 127:41-45 '193 patent at 128:61-65 '193 patent at 203:42-45 '193 patent at 267:34-42 '193 patent at 277:42-46 '193 patent at 281:36-39 See Control
environment 912.35, 900.155, 891.1, 683.2, 721.34	**Patent Specifications** '193 patent at 13:27-29 '193 patent at 17:1-6 '193 patent at 18:34-36 '193 patent at 25:39-43

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 36:26-29 '193 patent at 49:3-6 '193 patent at 49:15-17 '193 patent at 52:66-53:5 '193 patent at 69:33-35 '193 patent at 72:34-39 '193 patent at 73:40-42 '193 patent at 83:43-48 '193 patent at 100:10-16 '193 patent at 106:56-62 '193 patent at 141:43-45 '193 patent at 278:45-51 '900 patent at 245:23-39 '683 patent at 43:28-29 '721 patent at 1:21-28 '721 patent at 6:5-8 '721 patent at 6:66-7:7 **Extrinsic Sources** Webster's New World Dictionary of Computer Terms, 6th Edition (1997), p. 178. Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 178.
executable programming, executable 912.8, 912.35, 721.34	**Patent Specifications** '193 patent at 25:39-48 '193 patent at 25:57-60 '193 patent at 29:24-25 '193 patent at 73:30-31 '193 patent at 76:60-67 '193 patent at 77:32-36 '193 patent at 77:50-55 '193 patent at 78:6-7 '193 patent at 83:12-18 '193 patent at 83:43-48 '193 patent at 86:41-56 '193 patent at 110:60-111:8 '193 patent at 111:9-16 '193 patent at 111:20-34 '193 patent at 126:30-31 '193 patent at 136:52-55 '193 patent at 140:7-11 '193 patent at 141:42-56 '721 patent at 1:21-28 '721 patent at 5:34-39 '721 patent at 8:24-28 '912 patent at 329:16-24 **File Histories** '721 File History, 4/13/99 Amendment, p. 14. **Extrinsic Sources** Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 182.

Claim Term / Phrase	InterTrust Evidence
	Citations from Sources Designated by Microsoft under PLR 4-2(b) Krol, The Whole Internet: User's Guide and Catalog (O'Reilly, 1992), p. 69. IBM Dictionary of Computing (McGraw Hill, 1994), p. 250. Microsoft Computer Dictionary, 2nd ed. (Microsoft Press, 1994), p. 153. Encyclopedia of Computer Science and Engineering, 2nd ed. (Van Nostrand Reinhold, 1983), p. 1229.
execution space, execution space identifier 912.8	**Patent Specifications** '193 patent at 69:14-22 '193 patent at 69:33-35 '193 patent at 70:43-44 '193 patent at 75:38-42 '193 patent at 87:35-38 '193 patent at 88:38-43 '193 patent at 104:39-44 '193 patent at 105:55-57 '193 patent at 106:38-43 '193 patent at 107:31-47 '193 patent at 107:63-108:7 '193 patent at 109:27-33 '193 patent at 113:53-62 '193 patent at 140:15-141:11 '912 patent at 327:59-61 '912 patent at 327:65-67 '721 patent at 3:16-19 '721 patent at 4:51-54 '721 patent at 5:1-5 '721 patent at 8:34-40 **File Histories** '721 File History, 4/19/99 Amendment, p. 14.
governed item 683.2	**Patent Specifications** '683 patent at 24:33-39 '683 patent at 27:22-24 '193 patent at 9:27-31 '193 patent at 15:46-50 '193 patent at 33:26-30 '193 patent at 58:48-57 '193 patent at 63:39-44 '193 patent at 67:56-57 '193 patent at 76:37-41 '193 patent at 126:8-52 '193 patent at 128:41-46 '193 patent at 139:60-140:1 '193 patent at 159:23-26 '193 patent at 172:51-55 '193 patent at 174:15-29

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 241:17-26 '193 patent at 273:42-46 '193 patent at 288:11-12 '193 patent at 296:13-14 '193 patent at 312:63-66 **File Histories** '683 file history, 11/12/99 Office Action, p. 13. USP 6,389,402 File History, 12/6/00 Office Action, pp. 2-3. USP 6,363,488 File History, 12/19/00 Office Action, p. 2. USP 6,427,170 File History, 3/3/01 Office Action, p. 4. **Extrinsic Sources** Wyatt, Computer Professional's Dictionary (Osborne McGraw-Hill, 1990), p. 101. Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 131. The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 784. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Microsoft Computer Dictionary, 2nd ed. (Microsoft Press, 1994), pp. 107-108. Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 130. McNulty, Security on the Internet, Statement Before the Subcommittee on Science, Committee on Science, Space, and Technology, U S House of Representatives (Mar. 22, 1994), p. 9 ("Data Integrity - Verification that the contents of a data item (e.g., message, file, program) have not been accidentally or intentionally changed in an unauthorized manner").
halting 900.155	**Patent Specifications** '900 patent at 154:34-40 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 816. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Dictionary of Scientific and Technical Terms, 5th ed. (McGraw-Hill, 1994), p. 898. The American Heritage Dictionary of the English Language (1969), p. 595. Dictionary of Computing, 3rd ed. (Oxford, 1990), p. 201.
host processing environment 900.155	**Patent Specifications** '900 patent at 21:1-17 '900 patent at 49:31-48 '900 patent at 78:30-40 '900 patent at 87:32-46 '900 patent at 96:6-18 '900 patent at 112:2-27 '900 patent at 112:48-52 '193 patent at 13:7-23 '193 patent at 21:5-25

18

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 76:63-67 '193 patent at 79:30-46 '193 patent at 79:60-81:12 '193 patent at 83:47-48 '193 patent at 88:31-43 '193 patent at 104:39-64 '193 patent at 105:25-39 '193 patent at 203:63-65 '193 patent at 225:43-46 '683 patent at 20:16-19 '683 patent at 29:50-30:3
identifier, identify, identifying 193.11, 193.15, 912.8, 912.35, 861.58	**Patent Specifications** '193 patent at 25:31-38 '193 patent at 68:22-25 '193 patent at 85:59-63 '193 patent at 88:31-43 '193 patent at 131:33-45 '193 patent at 135:54-58 '193 patent at 140:35-50 '193 patent at 207:27-35 '193 patent at 233:35-41 '193 patent at 268:28-42 '193 patent at 270:12-21 '193 patent at 280:58-66 '193 patent at 298:45-54 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 896. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Cooper, Computer & Communications Security: Strategies for the 1990s, p. 375. Glossary of Telecommunications Terms (National Communications Systems, 1996), p. 1-1.
including 193.1 (at 320:63, and 321:3); 193.19 (at 324:15); 912.8 (at 327:36, 39, and 41); 912.35 (330:35 and 39); 861.58 (at 26:53 and 63); and 683.2 (at 63:60).	**Patent Specifications** '193 patent at 58:48-53 '193 patent at 126:62-65 '193 patent at 133:62-134:14 '193 patent at 136:53-56 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 913 **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Webster's College Dictionary of Random House (1991), p. 680. Funk & Wagnalls Standard College Dictionary (1973-74), p. 680. Random House Dictionary of the English Language: College Edition (1968), p. 673. Webster's Ninth New Collegiate Dictionary (Merriam-Webster, 1987), p. 609.

Claim Term / Phrase	InterTrust Evidence
information previously stored 900.155	**Patent Specifications** '900 patent at 239:15-55 '900 patent at 240:31-34 **Citations from Sources Designated by Microsoft under PLR 4-2(b)** The American Heritage Dictionary of the English Language (1969), p.1038. Webster's College Dictionary of Random House (1991), pp. 691, 1070.
integrity programming 900.155	**Patent Specifications** '900 patent at 228:28-39 '900 patent at 231:23-31 '900 patent at 233:8-15 '900 patent at 236:11-13 '900 patent at 236:31-38 '900 patent at 236:31-237:53 '900 patent at 239:4-240:6 '900 patent at 240:16-42 '900 patent at 243:29-41 '900 patent at 243:63-244:43 '900 patent at 246:52-247:57 **Citations from Sources Designated by Microsoft under PLR 4-2(b)** The New IEEE Standard Dictionary of Electrical and Electronic Terms (IEEE, 1993), pp. 304, 663. Russell et al., Computer Security Basics (O'Reilly & Associates, 1991), p. 414. Neumann, Computer Related Risks (ACM Press, 1995), p. 2.
key 193.19	**Patent Specifications** '193 patent at 12:35-39 '193 patent at 22:1-14 '193 patent at 49:3-4 '193 patent at 59:16-18 '193 patent at 67:26-31 '193 patent at 119:17-18 '193 patent at 129:30-35 '193 patent at 143:6-9 '193 patent at 200:1-9 '193 patent at 200:25-58 '193 patent at 201:50-55 '193 patent at 202:38-51 '193 patent at 207:50-60 '193 patent at 211:18-20 '193 patent at 211:30-216:21 **Extrinsic Sources** Mambo et al., A Tentative Approach to Constructing Tamper-Resistant Software, pp. 23-24. Parks, Microsoft Corporation, Microsoft® Windows Media™ Device Digital Rights Manager v7.1 (WM D-DRM): Overview And Design (WinHEC 2002 Presentation) slide 21. Davies, Security For Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer, Second Edition, (1984), p. 113.

Claim Term / Phrase	InterTrust Evidence
	Howard et al., Writing Secure Code, Microsoft Press (2002), p. 175
	Europay International S. A., MasterCard International Incorporated, and Visa International Service Association, Integrated Circuit Card Specification for Payment Systems (June 30, 1996), Page E-3
	The International Telegraph And Telephone Consultative Committee, Security Architecture For Open Systems Interconnection For Ccitt Applications, (1991), p.5
	Ehrsam et al., A cryptographic key management scheme for implementing the Data Encryption Standard, IBM Systems Journal 17, No. 2, 106-125, pp. 128-130.
	Banking – Personal Identification Number management and security – Part 1: PIN protection principles and techniques (International Organization of Standardization, ISO 9564-1 1991-12-15, First Edition) pp. 3 and 20.
	USP 4,168,396 (Best) at 2:7-9
	USP 5,509,070 (Schull) at 15:1-12
	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/diffie_hellman_keys.asp (Oct. 2002)
	Diffie and Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, v.!T-22, n.6 (Nov. 1976), pp. 644-654.
	Schneier, Applied Cryptography, 2nd ed. (Wiley, 1996), pp. 170-175, 189-211, 265-278, 397-398, 513-516.
	National Bureau of Standards, NBS FIPS PUB 81, DES Modes of Operation, US Department of Commerce (Dec. 1980).
	Telecom Glossary 2000, Technical Subcommittee on Performance and Signal Processing (American National Standard for Telecommunications, Feb. 2001), see entries for "derivation key," "key encrypting key pair," "key production key," "variant of a key," "key encrypting key," "master key," "linear key," "key type," "seed key." On the web at http://www.atis.org/tg2k/_derivation_key.html et seq.
	Citations from Sources Designated by Microsoft under PLR 4-2(b) National Information System Security (INFOSEC) Glossary, NSTISSI No. 4009 (Sept. 2000), p. 32.
	Glossary of Telecommunications Terms (National Communications Systems, 1996), pp. K-1, K-2, M-15.
	Shirey, Internet Security Glossary, Network Working Group, RFC 2828 (May 2000), p. 49.
	Freedman, The Computer Glossary: The Complete Illustrated Desk Reference, 6th ed. (Computer Language Co., 1992), p. 297.
	Pfleeger, Security in Computing (Prentice Hall, 1989), p. 398.
	Cooper, Computer & Communications Security: Strategies for the 1990s (Intertext Publications/Multiscience Press, 1989), pp. 334-335.

Claim Term / Phrase	InterTrust Evidence
load module 912.8, 721.1	**Patent Specifications** '193 patent at 17:15-21 '193 patent at 18:28-33 '193 patent at 25:39-52 '193 patent at 25:57-63 '193 patent at 34:26-37 '193 patent at 50:65 '193 patent at 71:26-31 '193 patent at 77:21-25 '193 patent at 85:21-29 '193 patent at 86:36-60 '193 patent at 110:60-67 '193 patent at 111:59-65 '193 patent at 126:15-31 '193 patent at 136:52-60 '193 patent at 139:14-142:38 '193 patent at 151:19-22 '721 patent at 3:21-35 '721 patent at 4:5-9 '721 patent at 4:22-42 '721 patent at 5:26-39 '721 patent at 14:39-60 **File Histories** 09/342,899 File History, 6/12/00 Office Action, p. 4 (citing USP 5,748,960 at 6:63-67); see also USP 5,748,960 at 1:33-52; 9:14-19; 11:15-25; 14:47-59; and 16:23-32. 09/328,668 File History, 5/16/01 Office Action, p. 4. **Extrinsic Sources** Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 287.
machine check programming 900.155	**Patent Specifications** '900 patent at 231:23-31 '900 patent at 233:8-15 '900 patent at 236:11-13 '900 patent at 236:31-237:53 '900 patent at 239:4-240:6 '900 patent at 240:16-42 '900 patent at 243:29-41 '900 patent at 243:63-244:43 '900 patent at 246:52-247:57
opening secure containers 683.2	**Patent Specifications** '683 patent at 8:28-31 '683 patent at 9:59-61 '683 patent at 13:6 '683 patent at 15:67-16:4 '683 patent at 18:42-49 '683 patent at 42:34-52 '683 patent at 49:31-38 '683 patent at 56:17-25 '193 patent at 183:24-25 '193 patent at 184:6-22

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 185:11-12 '193 patent at 254:45-46 **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Encyclopedia of Computer Science and Engineering, 2nd ed. (Van Nostrand Reinhold, 1983), p. 1051.
operating environment 891.1	**Patent Specifications** '193 patent at 34:37-41 '193 patent at 34:54-59 '193 patent at 63:13-17 **Extrinsic Sources** Webster's New World Dictionary of Computer Terms, 6th ed. (1997), p. 370.
organization, organization information, organize 861.58	**Patent Specifications** '861 patent at 5:57-6:7 '861 patent at 7:54-58 '861 patent at 10:38-53 '861 patent at 14:14-29 '861 patent at 28:34-43 '861 patent, Abstract '193 patent at 33:43-49 '193 patent at 103:23-32 '193 patent at 127:17-19 '193 patent at 232:63-233:1 '193 patent at 274:54-58 '193 patent at 294:41-45 '193 patent at 302:2-12 '193 patent at 309:4-9
portion 193.1, 193.11, 193.15, 193.19, 912.8, 912.35, 861.58	**Patent Specifications** '193 patent at 23:66-24:2 '193 patent at 24:41-43 '193 patent at 46:22-24 '193 patent at 59:34-37 '193 patent at 128:49-55 '193 patent at 226:14-16 '193 patent at 299:19-31 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 1412. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Webster's College Dictionary of Random House (1991), p. 1052. Funk & Wagnalls Standard College Dictionary (1973-74), p. 1052.
prevents 721.34	**Patent Specifications** '721 patent at 6:56-62 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 1436. **Citations from Sources Designated by Microsoft under PLR 4-2(b)**

Claim Term / Phrase	InterTrust Evidence
	Webster's College Dictionary of Random House (1991), p. 1070. Random House Dictionary of the English Language: College Edition (1968), p. 1050.
processing environment 912:35, 900:155, 721:34, 683.2	**Patent Specifications** '193 patent at 13:17-23 '193 patent at 75:65-76:9 '193 patent at 79:36-39 '721 patent at 1:21-28 **File Histories** USP 5,915,019 File History, 4/15/98 Office Action, p. 4. **Extrinsic Sources** Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 383. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** IBM Dictionary of Computing (McGraw Hill, 1994), p. 533.
protected processing environment 721:34, 683.2	**Patent Specifications** '193 patent at 13:7-14 '193 patent at 13:17-23 '193 patent at 79:24-83:9 '193 patent at 105:15-41 '193 patent at 223:30-225:19 '193 patent at 226:43-57 '193 patent at 277:26-32 '193 patent at 278:45-65 '193 patent at 283:44-46 '193 patent at 291:39-49 '193 patent at 298:9-10 '193 patent at 318:1-5 '683 patent at 12:59-61 '683 patent at 16:60-62 '683 patent at 29:51-30:3 '721 patent at 3:16-21 '721 patent at 8:33-40 **File Histories** '721 File History, 4/13/99 Amendment, p. 13.
protecting 683.2	**Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 1456.
record (n.) 912.8, 912.35	**Patent Specifications** '193 patent at 134:54-58 '193 patent at 138:12-139:13 '193 patent at 264:20-57 '193 patent at 324:64-67 **File Histories** '912 File History, 12/24/97 Office Action, pp. 2-3 (citing USP 5,629,980); see also

Claim Term / Phrase	InterTrust Evidence
	USP 5,629,980 at 9:6-11:29. '912 File History, 6/24/98 Amendment, pp. 73-74. '912 File History, 9/22/98 Office Action, pp. 2-3 (citing USP 5,748,960); see also USP 5,748,960 at 11:7-13 and 12:46-48). **Extrinsic Sources** Personal Computer Dictionary (1995), p. 149. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** The New IEEE Standard Dictionary of Electrical and Electronic Terms (IEEE, 1993), p. 1087. Hutt et al., Computer Security Handbook, 2nd ed. (1987), p. 389. Telecommunications: Glossary of Telecommunications Terms (National Communications Systems, 1996), p. R-10. Hansen, The Dictionary of Computing and Digital Media: Terms and Acronyms (1999), p. 261. Dictionary of Scientific and Technical Terms, 5th ed. (McGraw-Hill, 1994), p. 1664. Illustrated Dictionary of Computing, 2nd ed. (Prentice Hall, 1992), p. 505. Laplante, Dictionary of Computer Science, Engineering and Technology (2001), p. 410. Webster's New World Dictionary of Computer Terms, 4th ed. (1992), p. 349. Longley et al., Information Security: Dictionary of Concepts, Standards and Terms (Stockton Press, 1992), p.437. IBM Dictionary of Computing (McGraw Hill, 1994), p. 561. Encyclopedia of Computer Science and Engineering, 2nd ed. (Van Nostrand Reinhold, 1983), p. 1272.
required 912.8, 861.58	**Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 1533. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Random House Dictionary of the English Language: College Edition (1968), p. 1121.
resource processed 891.1	**Patent Specifications** '193 patent at 7:48-57 '193 patent at 21:5-25 '193 patent at 29:3-8 '193 patent at 38:60-39:8 '193 patent at 40:1-7 '193 patent at 57:49-51 '193 patent at 64:2-5 '193 patent at 69:63-65 '193 patent at 51:61 '193 patent at 72:39-44 '193 patent at 74:28-37 '193 patent at 75:5-8

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 75:15-30 '193 patent at 75:42-47 '193 patent at 76:61-77:11 '193 patent at 77:57-63 '193 patent at 79:36-39 '193 patent at 79:50-54 '193 patent at 79:64-67 '193 patent at 80:9-12 '193 patent at 80:30-35 '193 patent at 81:14-19 '193 patent at 81:32-35 '193 patent at 88:50-52 '193 patent at 89:49-55 '193 patent at 90:31-46 '193 patent at 91:12-25 '193 patent at 94:14-18 '193 patent at 100:32-35 '193 patent at 100:46-54 '193 patent at 101:38-42 '193 patent at 104:49-52 '193 patent at 104:59-64 '193 patent at 108:1-4 '193 patent at 141:49-55 '193 patent at 201:47-49 '193 patent at 201:57-58 '193 patent at 241:52-55 '193 patent at 252:60-62 '193 patent at 258:45-52 '193 patent at 276:53-58 '193 patent at 282:20-24 '193 patent at 283:23-28 '193 patent at 283:40-44 '193 patent at 284:16-28 '193 patent at 313:3-18 '193 patent at 314:33-39 **File Histories** '891 File History, 12/20/96 Office Action, p. 2. USP 6,363,488 File History, 12/19/00 Office Action, p. 2.
rule 861.58, 683.2	**Patent Specifications** '683 patent at 6:11-22 '683 patent at 11:37-38 '683 patent at 15:22 '683 patent at 24:26-33 '683 patent at 45:60-63 '683 patent at 47:42-45 '683 patent at 54:29-37 '683 patent at 55:23-26 '193 patent at 53:53-59 '193 patent at 59:1-5 '193 patent at 149:24-40 '193 patent at 241:11-14 '193 patent at 241:29-36 '193 patent at 242:9-61

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 243:4-7 '193 patent at 243:57-62 '193 patent at 253:9-30 '193 patent at 253:34-40 '193 patent at 253:46-49 '861 patent at 1:53-60 '861 patent at 2:13-36 '861 patent at 6:19-23 '861 patent at 15:66-16:9 '861 patent at 18:26-44 '861 patent at 20:38-51 '861 patent, Abstract **File Histories** '683 File History, 11/12/99 Office Action, pp. 4, 6 (citing USP 5,412,717 at 10:8-39); see also USP 5,412,717 at 2:24-48 and 12:24-44. USP 6,427,140 File History, 3/30/01 Office Action, pp. 3-4. USP 6,138,119 File History, 10/26/99 Office Action, p. 4. USP 6,138,119 File History, 4/26/00 Office Action, p. 9. App. No. 09/498,369, 5/30/02 Office Action, p. 3 (citing 5,765,152 patent at 4:61-5:4). USP 6,389,402 File History, 12/6/00 Office Action, pp. 2-3, 6 (citing USP 3,790,700 and USP 5,629,980 at 23:37-42); see also USP 3,790,700 at 5:14-18, 35-46; and USP 5,629,980 at 23:9-42.
secure 193.1, 193.11, 193.15, 912.35, 861.58, 891.1, 683.2, 721.34	**Patent Specifications** '193 patent at 8:1-7 '193 patent at 12:33-39 '193 patent at 13:54-57 '193 patent at 17:33-37 '193 patent at 17:67-18:5 '193 patent at 21:26-29 '193 patent at 22:15-19 '193 patent at 41:37-42 '193 patent at 42:8-16 '193 patent at 45:19-32 '193 patent at 45:39-45 '193 patent at 45:52-59 '193 patent at 46:4-5 '193 patent at 49:33-55 '193 patent at 49:59-62 '193 patent at 59:48-59 '193 patent at 63:35-39 '193 patent at 63:48-64:47 '193 patent at 68:66-69:22 '193 patent at 71:31-40 '193 patent at 73:19-37 '193 patent at 81:12-19 '193 patent at 77:30-78:18 '193 patent at 80:22-81:19 '193 patent at 83:44-48 '193 patent at 84:60-85:2 '193 patent at 87:33-66

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 88:36-43 '193 patent at 125:60-64 '193 patent at 126:6-8 '193 patent at 126:30-32 '193 patent at 199:36-200:9 '193 patent at 200:66-201:4 '193 patent at 203:58-204:2 '193 patent at 216:22-217:12 '193 patent at 221:1-37 '193 patent at 226:55-56 '193 patent at 233:25-30 '193 patent at 233:51-54 '193 patent at 238:46-65 '721 patent at 1:19-28 **File Histories** App. No. 09/328,668, 5/16/01 Office Action, p. 2 (citing USP 5,388,211 at 5:35-40). '683 File History, 11/12/99 Office Action, p. 11. **Extrinsic Sources** Webster's New World Dictionary of Computer Terms, 6th Edition (1997), p. 463. **Citations from Citations from Sources Designated by Microsoft under PLR 4-2(b)** The New IEEE Standard Dictionary of Electrical and Electronic Terms (IEEE, 1993), p. 1181. Cooper, Computer & Communications Security: Strategies for the 1990s, p. 383. Freedman, The Computer Glossary: The Complete Illustrated Desk Reference (Computer Language Co., 1992), p. 460. Dictionary of Computing, 3rd ed. (Oxford, 1990), p. 406. Encyclopedia of Computer Science and Engineering, 2nd ed. (Van Nostrand Reinhold, 1983), pp. 493-497. Landwehr, Formal Models for Computer Security, ACM Computer Surveys (Sept. 3, 1981), pp. 247, 253. Mullender, Distributed Systems, 2nd ed. (Addison-Wesley, 1993), p. 420. Hutt et al., Computer Security Handbook, pp. 75, 201, 218, 221, 292-93. Hoffman, Modern Methods for Computer Security and Privacy (Prentice-Hall, 1977), p. 170. Garfinkel et al., Practical Unix Security (O'Reilly & Associates, 1991), pp. 12-13. Neumann, Computer Related Risks (ACM Press, 1995), pp. 2, 96. Tanenbaum, Modern Operating Systems (Prentice Hall, 1992), p. 182.
secure container	**Patent Specifications** '683 patent at 7:10-13 '683 patent at 9:59-61

Claim Term / Phrase	InterTrust Evidence
912.35, 861.58, 683.2	'683 patent at 15:61-16:4 '683 patent at 18:49-56 '683 patent at 25:29-34 '683 patent at 25:62-26:4 '683 patent at 29:64-66 '683 patent at 53:3-5 '193 patent at 8:1-7 '193 patent at 8:53-66 '193 patent at 12:40-43 '193 patent at 13:44-14:4 '193 patent at 15:39-46 '193 patent at 17:46-55 '193 patent at 19:15-32 '193 patent at 22:20-25 '193 patent at 24:64-25:2 '193 patent at 31:66-32:3 '193 patent at 33:24-26 '193 patent at 34:13-49 '193 patent at 43:26-32 '193 patent at 52:55-56 '193 patent at 58:37-59:5 '193 patent at 103:47-58 '193 patent at 104:12-28 '193 patent at 126:15-28 '193 patent at 127:2-134:23 '193 patent at 128:11-21 '193 patent at 189:25-29 '193 patent at 241:5-15 '193 patent at 264:40-49 '193 patent at 274:54-61 '193 patent at 277:13-15 '193 patent at 284:8-16 '193 patent at 291:29-33 '193 patent at 292:27-47 '193 patent at 301:36-57 '193 patent at 313:33-36 '193 patent at 314:43-49 '193 patent at 317:57-318:8 '861 patent at 2:12-16 '861 patent at 5:26-30 '861 patent at 6:24-29 **Extrinsic Sources** USP 5,634,019 at 7:34-49 Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 115. **File Histories** '683 File History, 11/12/99 Office Action, p. 4, 6, 12 (citing USP 5,412,717); see also USP 5,412,717 at 5:3-37. '861 File History, 6/25/98 Office Action, p. 5 (citing USP 5,537,526); see also USP 5,537,526 at 15:63-16:25. USP 6,363,488 File History, 12/19/00 Office Action, pp. 3-4.

Claim Term / Phrase	InterTrust Evidence
	USP 6,237,786 File History, 7/17/00 Office Action, pp. 2-3 (citing USP 4,817,508); see also USP 4,817,508 at 8:61-9:2; 9:32-36; 19:8-26; and 21:39-55. 09/764,370 File History, 1/18/01 Amendment, pp. 17-19. USP 6,427,140 File History, 3/30/01 Office Action, p. 3. 09/819,063 File History, 9/27/00 Preliminary Amendment, pp. 21-22. 09/498,369 File History, 5/30/02 Office Action, p. 3 (citing USP 5,765,152 at 4:61-5:4); see also USP 5,765,152 at Fig. 7D. USP 6,112,181 File History, 12/31/98 Office Action, p. 15 (citing USP 5,740,549 at 16:45-54). USP 5,915,019 File History, 4/15/98 Office Action, pp. 3-4 (citing USP 5,311,591 at 2:14-46).
secure container governed item 683.2	**Patent Specifications** '193 patent at 58:38-58
secure database 193.1, 193.11, 193.15	**Patent Specifications** '193 patent at 50:54-55 '193 patent at 51:11-40 '193 patent at 62:66-63:7 '193 patent at 69:56-62 '193 patent at 71:28-40 '193 patent at 72:14-25 '193 patent at 88:27-28 '193 patent at 90:16-20 '193 patent at 100:21-101:31 '193 patent at 157:24-30 '193 patent at 120:59-66 '193 patent at 123:64-125:2 '193 patent at 126:6-67 '193 patent at 142:67-143:46 '193 patent at 148:34-43 '193 patent at 153:33-154:49 '193 patent at 156:26-169:18 '193 patent at 205:60-64 '193 patent at 211:3-9 '193 patent at 215:34-43 '193 patent at 215:58-218:30 '193 patent at 226:26-42 **File Histories** 09/342,899 File History, 6/12/00 Office Action, pp. 4-5. '193 File History, 6/7/00 Office Action, p. 2 (citing USP 4,595,950); see also USP 4,595,950 at 4:38-54; 8:52-68; and 14:49-15:11. '683 File History, 11/12/99 Office Action, pp. 5-6.

Claim Term / Phrase	InterTrust Evidence
	'900 File History, 8/27/98 Office Action, p. 7 (citing USP 5,048,085 at 6:55-7:14). '900 File History, 12/9/97 Office Action, pp. 5, 10 (citing USP 5,655,077 at 3:60-67 and USP 5,572,673); see also USP 5,655,077 at 4:24-59; and USP 5,572,673, Abstract. **Extrinsic Sources** Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 129. Wyatt, Computer Professional's Dictionary (Osborne McGraw-Hill, 1990), p. 98. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Encyclopedia of Computer Science and Engineering, 2nd ed. (Van Nostrand Reinhold, 1983), p. 441. Hansen, The Dictionary of Computing and Digital Media: Terms and Acronyms (1999), p. 74.
secure execution space 721.34	**Patent Specifications** '721 patent at 6:34-41 '721 patent at 6:49-52 '721 patent at 7:14-25 '721 patent at 8:33-40
secure memory, memory 193.1, 193.11, 193.15	**Patent Specifications** '193 patent at 13:7-14 '193 patent at 21:17-42 '193 patent at 22:15-19 '193 patent at 23:43-50 '193 patent at 32:15-21 '193 patent at 49:15-17 '193 patent at 49:33-55 '193 patent at 59:42-59 '193 patent at 60:1-3 '193 patent at 62:14-24 '193 patent at 62:43-57 '193 patent at 63:60-64:5 '193 patent at 65:64-66:4 '193 patent at 69:14-22 '193 patent at 69:25-51 '193 patent at 69:54-59 '193 patent at 69:65-71:47 '193 patent at 71:48-60 '193 patent at 72:52-73:22 '193 patent at 79:60-81:11 '193 patent at 81:12-19 '193 patent at 88:62-66 '193 patent at 104:49-64 '193 patent at 109:24-60 '193 patent at 110:47-49 '193 patent at 111:12-16 '193 patent at 120:60-63 '193 patent at 121:41-43 '193 patent at 125:60-67 '193 patent at 169:3-12 '193 patent at 206:8-11 '193 patent at 216:56-217:20 '193 patent at 218:4-15

Claim Term / Phrase	InterTrust Evidence
	File Histories '900 File History, 6/9/98 Amendment, pp. 7-8. '900 File History, 8/27/98 Office Action, p. 3 (citing USP 5,048,085 at 6:61-7:14). 09/698,044 File History, 10/27/00 Amendment, p. 14. 09/272,998 File History, 10/11/01 Office Action, p. 3. **Extrinsic Sources** Microsoft Computer Dictionary, 3rd ed. (Microsoft Press, 1997), p. 302. The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), pp. 1126, 1631-1632. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Cooper, Computer & Communications Security: Strategies for the 1990s, p. 386. Hansen, The Dictionary of Computing and Digital Media: Terms and Acronyms (1999), p. 329. Dictionary of Scientific and Technical Terms, 5th ed. (McGraw-Hill, 1994), p. 2136. Webster's Ninth New Collegiate Dictionary (Merriam-Webster, 1987), p. 1317. Encyclopedia of Computer Science and Engineering, 2nd ed. (Van Nostrand Reinhold, 1983), p. 968.
secure operating environment, said operating environment 891.1	**Patent Specifications** '193 patent at 13:37-41 '193 patent at 69:33-35 '193 patent at 83:44-48 **File Histories** '912 File History, 12/24/97 Office Action, p. 3.
securely applying 891.1	**Patent Specifications** '193 patent at 9:40-45 '193 patent at 18:60-19:1 '193 patent at 19:13-21 '193 patent at 22:48-58 '193 patent at 26:59-67 '193 patent at 28:8-15 '193 patent at 30:38-41 '193 patent at 30:55-65 '193 patent at 33:10-24 '193 patent at 33:30-37 '193 patent at 43:41-43 '193 patent at 45:7-9 '193 patent at 54:36-38 '193 patent at 57:27-28 '193 patent at 59:34-37 '193 patent at 120:15-18 '193 patent at 283:33-39 '193 patent at 299:19-51 '193 patent at 300:6-30

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 308:1-7
securely assembling 912.8, 912.35	**Patent Specifications** '193 patent at 25:57-26:12 '193 patent at 83:43-85:39 '193 patent at 86:66-88:21 '193 patent at 112:46-113:62 '193 patent at 115:43-116:51 '193 patent at 126:34-36 '193 patent at 138:32-36 '193 patent at 159:61-160:8 '193 patent at 250:21-34 '193 patent at 260:36-47
securely processing 891.1	**Patent Specifications** '193 patent at 79:24-81:12 '193 patent at 104:39-64 '193 patent at 105:15-20 **File Histories** '900 File History, 12/9/97 Office Action, p. 6 (citing USP 5,486,622); see also USP 5,486,622, Abstract.
securely receiving 891.1	**Patent Specifications** '193 patent at 5:4-6 '193 patent at 12:33-39 '193 patent at 13:54-57 '193 patent at 55:52-54 '193 patent at 57:27-36 '193 patent at 60:33-48 '193 patent at 62:32-39 '193 patent at 67:21-52 '193 patent at 68:65-69:11 '193 patent at 75:65-76:1 '193 patent at 76:10-32 '193 patent at 77:30-44 '193 patent at 81:26-32 '193 patent at 83:53-84 '193 patent at 91:38-51 '193 patent at 96:1-5 '193 patent at 96:12-17 '193 patent at 101:54-102:25 '193 patent at 102:41-51 '193 patent at 104:29-37 '193 patent at 118:64-119:42 '193 patent at 123:22-28 '193 patent at 123:50-56 '193 patent at 155:51-156:2 '193 patent at 160:65-161:51 '193 patent at 162:39-65 '193 patent at 162:66-163:35 '193 patent at 200:66-201:42 '193 patent at 211:39-212:10 '193 patent at 214:57-67 '193 patent at 218:31-220:19

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 225:50-226:36 '193 patent at 227:25-228:30 '193 patent at 233:25-32 '193 patent at 282:56-61 '193 patent at 283:61-65 '193 patent at 290:46-62 '891 patent at 322:56-63 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 1508.
security level, level of security 721.1; 721.34, 912.8	**Patent Specifications** '721 patent at 6:16-62 '721 patent at 16:38-17:5 '721 patent at 17:24-40 '721 patent at 18:44-19:10 '721 patent at 19:24-32 '193 patent at 140:15-141:11
tamper resistance 721.1, 721.34, 900.155	**Patent Specifications** '721 patent at 3:16-19 '721 patent at 4:40-42 '721 patent at 5:1-6 '721 patent at 6:25-30 '721 patent at 6:34-41 '721 patent at 6:53-56 '721 patent at 16:38-17:5 '193 patent at 20:53-57 '193 patent at 21:23-37 '193 patent at 22:1-6 '193 patent at 49:15-31 '193 patent at 59:48-59 '193 patent at 63:60-64:5 '193 patent at 73:30-31 '193 patent at 77:34-38 '193 patent at 80:22-81:11 '193 patent at 87:41-60 '193 patent at 110:47-49 '193 patent at 114:57-62 '193 patent at 120:59-121:1 '193 patent at 130:28-33 '193 patent at 218:33-63 '683 patent at 3:27-34 '683 patent at 5:11-17 '683 patent at 8:9-10 '683 patent at 16:58-62 '683 patent at 20:16-19 '683 patent at 29:55-30:3 **File Histories** '900 File History, 12/9/97 Office Action, p. 9 (citing USP 4,864,494, Abstract; 4:13-40; 6:21-65; and 7:15-47).

Claim Term / Phrase	InterTrust Evidence
	'900 File history, 8/27/98 Office Action, p. 3 (citing USP 5,048,085); see also USP 5,048,085 at 6:55-7:19 USP 5,917,912 File History, 9/22/98 Office Action, p. 4. '683 File History, 11/12/99 Office Action, p. 5 (citing USP 5,499,298, Abstract and 6:45-7:9). **Extrinsic Sources** Kent, Protecting Externally Supplied Software in Small Computers, Doctoral Thesis (Sept. 22, 1980), p. PA00000362. Aucsmith, Tamper Resistant Software: An Implementation (1996), p. PA00002323 Mambo et al., A Tentative Approach to Constructing Tamper-Resistant Software, School of Information Science, Japan Advanced Institute of Science and Technology, 1-1 Asahidai Tatsunokuchi Nomi, Ishikawa, p. PA00005363 USP 5,594,227 at 2:42-48. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Hensley et al., SCP Software Protection User's Guide (Sept. 18, 2000), pp. MSI140484 - MSI140485.
tamper resistant barrier 721.34	**Patent Specifications** '721 patent at 5:1-6 '193 patent at 59:48-59 '193 patent at 63:47-64:5 '193 patent at 64:13-31 '193 patent at 71:32-40 '193 patent at 79:49-50 '193 patent at 80:22-65 **File Histories** '721 File History, 4/13/99 Amendment, p. 14. 09/272,998 File History, 10/11/01 Office Action, p. 3. '900 File History, 8/27/98 Office Action, p. 3.
tamper resistant software 900.155	**Patent Specifications** '900 patent at 87:61-88:33 '900 patent at 230:57-65 '900 patent at 233:24-33 '900 patent at 235:27-236:29 '683 patent at 29:50-30:3 **Extrinsic Sources** Aucsmith, Tamper Resistant Software: An Implementation (1996), p. PA00002323 Mambo et al., A Tentative Approach to Constructing Tamper-Resistant Software, School of Information Science, Japan Advanced Institute of Science and Technology, 1-1 Asahidai Tatsunokuchi Nomi, Ishikawa, p. PA00005363 USP 5,991,399 at 4:14-23; 5:47-55.

Claim Term / Phrase	InterTrust Evidence
use 912.8, 912.35, 861.58, 193.19, 891.1, 683.2, 721.1	**Patent Specifications** '683 patent at 63:35-67 '193 patent at 324:8-37 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 1966.
user controls 683.2	**File Histories** '683 File History, 11/12/99 Office Action, p. 4.
validity 912.8	**Patent Specifications** '193 patent at 38:27-29 '193 patent at 41:37-42 '193 patent at 67:56-60 '193 patent at 77:30-41 '193 patent at 78:6-14 '193 patent at 85:42-67 '193 patent at 87:52-62 '193 patent at 111:59-112:12 '193 patent at 112:37-59 '193 patent at 119:66 '193 patent at 120:59-121:3 '193 patent at 137:54-67 '193 patent at 152:10-37 '193 patent at 152:40-153:8 '193 patent at 157:42-45 '193 patent at 157:57-67 '193 patent at 164:35-40 '193 patent at 217:51-52 '193 patent at 218:1-15 '193 patent at 220:47-52 '193 patent at 318:59-62
virtual distribution environment 900.155	**Patent Specifications** '900 patent at 2:19-31 '900 patent at 2:51-56 '900 patent at 3:18-45 '900 patent at 3:60-4:4 '900 patent at 4:10-13 '900 patent at 4:45-5:45 '900 patent at 6:29-42 '900 patent at 7:10-12 '900 patent at 7:34-8:7 '900 patent at 8:58-9:2 '900 patent at 9:8-58 '900 patent at 11:36-47 '900 patent at 13:26-49 '900 patent at 13:58-62 '900 patent at 21:41-46 '900 patent at 43:43-46 '900 patent at 43:57-44:6 '900 patent at 46:48-52 '900 patent at 48:65-49:2 '900 patent at 50:1-3 '900 patent at 50:30-32 '900 patent at 53:39-54:36

Claim Term / Phrase	InterTrust Evidence
	'900 patent at 55:63-56:5 '900 patent at 56:66-57:8 '900 patent at 57:15-17 '900 patent at 61:19-21 '900 patent at 87:61-88:47 '900 patent at 280:9-46 '900 patent at 302:17-24 '900 patent at 303:40-61 '900 patent at 316:36-45 '900 patent, Abstract '193 patent at 13:46-50 '193 patent at 13:54-57 '193 patent at 16:49-56 **File Histories** '721 File History, 4/13/99 Amendment, p. 13. '891 File History, 9/25/96 Office Action, pp. 1-3. '891 File History, 6/20/97 Amendment, p. 1. USP 5,915,019 File History, 1/8/97 Amendment, p. 1.
'193:1	
receiving a digital file including music	**Patent Specifications** '193 patent at 1:46-52 '193 patent at 1:61-63 '193 patent at 3:26-29 '193 patent at 9:13-19 '193 patent at 12:5-39 '193 patent at 12:47-13:6 '193 patent at 13:54-14:28 '193 patent at 14:31-48 '193 patent at 16:25-40 '193 patent at 17:46-56 '193 patent at 18:10-14 '193 patent at 18:61-64 '193 patent at 22:1-14 '193 patent at 21:52-53; 23:51-24:14; 24:57-25:30 '193 patent at 38:43-55 '193 patent at 45:19-27 '193 patent at 45:39-45 '193 patent at 46:5-8 '193 patent at 52:66-53:8 '193 patent at 53:13-22 '193 patent at 53:33-37 '193 patent at 53:45-59 '193 patent at 54:51-58 '193 patent at 55:21-56:24 '193 patent at 57:33-39 '193 patent at 58:59-64 '193 patent at 59:39-42 '193 patent at 60:37-48 '193 patent at 62:27-42 '193 patent at 63:32-39 '193 patent at 64:48-51

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 65:8-14
	'193 patent at 67:31-52
	'193 patent at 68:65-69:12
	'193 patent at 74:51-53
	'193 patent at 75:23-28
	'193 patent at 75:65-76:32
	'193 patent at 81:26-32
	'193 patent at 83:53-63
	'193 patent at 90:1-33
	'193 patent at 90:38-46
	'193 patent at 91:26-51
	'193 patent at 96:1-7
	'193 patent at 96:12-24
	'193 patent at 98:66-99:3
	'193 patent at 99:28-35
	'193 patent at 101:54-102:61
	'193 patent at 104:29-37
	'193 patent at 105:23-39
	'193 patent at 115:13-21
	'193 patent at 115:26-29
	'193 patent at 123:51-55
	'193 patent at 130:13-54
	'193 patent at 133:39-134:23
	'193 patent at 135:31-42
	'193 patent at 153:53-156:47
	'193 patent at 161:7-162:65
	'193 patent at 170:41-172:13
	'193 patent at 172:61-177:53
	'193 patent at 178:49-179:55
	'193 patent at 214:59-67
	'193 patent at 218:33-220:19
	'193 patent at 220:53-67
	'193 patent at 222:4-11
	'193 patent at 225:22-226:36
	'193 patent at 227:25-45
	'193 patent at 231:32-59
	'193 patent at 233:25-47
	'193 patent at 234:36-43
	'193 patent at 234:65-235:1
	'193 patent at 235:13-38
	'193 patent at 243:51-244:48
	'193 patent at 254:30-34
	'193 patent at 254:59-65
	'193 patent at 264:29-49
	'193 patent at 266:52-267:45
	'193 patent at 273:42-53
	'193 patent at 277:10-17
	'193 patent at 279:42-53
	'193 patent at 282:10-61
	'193 patent at 283:23-28
	'193 patent at 283:56-284:42
	'193 patent at 288:43-60
	'193 patent at 289:14-27
	'193 patent at 290:30-62
	'193 patent at 313:33-41
	'193 patent at 313:58-67
	'193 patent at 315:24-28

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 316:1-6 '193 patent at 316:16-317:19 '193 patent, Figs. 1, 1A, 2, 2A, 3, 7, 8, 9, 9A, 10, 12, 13, 16, 19, 20, 21, 27, 28, 30, 31, 35, 36, 37, 38, 41a, 41b, 41c, 41d, 67, 69, 69A, 70, 71, 74, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, and 87 See "Receiving a digital file" (193.11); Securely Receiving **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 1508.
a budget specifying the number of copies which can be made of said digital file	**Patent Specifications** '193 patent at 48:29-35 '193 patent at 133:39-50 '193 patent at 143:38-144:32 '193 patent at 162:39-65 '193 patent at 172:61-174:29 '193 patent at 220:20-40 See "Digital file versus a copy," below.
controlling the copies made of said digital file	**Patent Specifications** '193 patent at 48:29-35 '193 patent at 81:4-12 '193 patent at 102:26-40 '193 patent at 133:39-134:23 '193 patent at 140:37-50 '193 patent at 143:39-144:31 '193 patent at 172:18-48 '193 patent at 172:61-174:29 '193 patent at 203:58-67 '193 patent at 212:65-213:36 '193 patent at 229:45-232:3 '193 patent at 235:39-236:25 '193 patent at 263:46-264:4 '193 patent at 279:42-60 See Protected Processing Environment
determining whether said digital file may be copied and stored on a second device based on at least said copy control	**Patent Specifications** '193 patent at 48:12-35 '193 patent at 102:26-40 '193 patent at 133:39-50 '193 patent at 220:20-40 '193 patent at 263:46-264:57 '193 patent at 265:9-38 '193 patent at 278:9-25 '193 patent at 279:42-60 '193 patent at 316:16-317:19 '193 patent at 322:65-66 '193 patent at 323:4-7 '193 patent at 323:50-324:7 '193 patent at 325:32-35
if said copy control allows at least a portion of said digital file to be copied and stored on a second	**Patent Specifications** '193 patent at 48:12-35 '193 patent at 102:26-40

Claim Term / Phrase	InterTrust Evidence
device	'193 patent at 133:39-50 '193 patent at 220:20-40 '193 patent at 263:46-264:57 '193 patent at 265:9-37 '193 patent at 278:9-25 '193 patent at 279:42-60 '193 patent at 316:16-317:19 '193 patent at 322:65-66 '193 patent at 323:4-7 '193 patent at 325:32-35
copying at least a portion of said digital file	**Patent Specifications** '193 patent at 48:12-34 '193 patent at 133:39-50 '193 patent at 220:20-40 '193 patent at 264:28-57 '193 patent at 278:9-25 '193 patent at 316:16-317:19 '193 patent at 322:65-66 '193 patent at 323:4-7 '193 patent at 325:32-35
transferring at least a portion of said digital file to a second device	**Patent Specifications** '193 patent at 38:4-9 '193 patent at 48:12-43 '193 patent at 65:24-38 '193 patent at 68:51-61 '193 patent at 72:1-9 '193 patent at 133:39-50 '193 patent at 162:10-15 '193 patent at 167:41-43 '193 patent at 220:21-40 '193 patent at 226:11-16 '193 patent at 237:34-47 '193 patent at 252:51-58 '193 patent at 264:28-57 '193 patent at 278:9-25 '193 patent at 316:16-317:19 '193 patent at 322:65-66 '193 patent at 323:4-7 '193 patent at 324:8-37 '193 patent at 325:32-40 See "Storing information associated with said digital file in a secure database stored on said first device, said information including at least one control" (193.15)
storing said digital file	**Patent Specifications** '193 patent at 88:24-30 '193 patent at 99:7-16 '193 patent at 102:43-62 '193 patent at 127:41-62 '193 patent at 134:10-14 '193 patent at 153:50-154:16 '193 patent at 229:45-231:31 '193 patent at 289:5-8 '193 patent at 289:14-19

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 289:65-66
'193:11	
receiving a digital file	**Patent Specifications** '193 patent at 52:66-53:8 '193 patent at 55:39-56 '193 patent at 60:37-48 '193 patent at 102:41-61 '193 patent at 133:39-134:23 '193 patent at 282:29-61 '193 patent at 316:16-317:19 '193 patent at 323:14-40 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 1508. See "Receiving a digital file including music" ('193.1)
determining whether said digital file may be copied and stored on a second device based on said first control	See "Determining whether said digital file may be copied and stored on a second device based on at least said copy control" ('193.1).
identifying said second device	**Patent Specifications** '193 patent at 42:8-20 '193 patent at 47:49-57 '193 patent at 81:4-11 '193 patent at 203:58-67 '193 patent at 212:65-213:36 '193 patent at 230:22-27 '193 patent at 279:42-60 See Identify and Identifier
whether said first control allows transfer of said copied file to said second device	**Patent Specifications** '193 patent at 48:28-34 '193 patent at 102:26-40 '193 patent at 263:46-264:49 '193 patent at 265:9-38 '193 patent at 279:42-60 '193 patent at 316:16-317:19 See "Determining whether said digital file may be copied and stored on a second device based on at least said copy control" ('193.1)
said determination based at least in part on the features present at the device	**Patent Specifications** '193 patent at 42:8-20 '193 patent at 47:49-57 '193 patent at 81:4-11 '193 patent at 203:58-67 '193 patent at 212:65-213:36 '193 patent at 230:22-27 '193 patent at 279:42-60
if said first control allows at least	**Patent Specifications**

Claim Term / Phrase	InterTrust Evidence
a portion of said digital file to be copied and stored on a second device	'193 patent at 48:28-35 '193 patent at 102:26-40 '193 patent at 263:46-264:57 '193 patent at 265:9-38 '193 patent at 279:42-60 '193 patent at 316:16-317:19 See "If said copy control allows at least a portion of said digital file to be copied and stored on a second device" ('193.1).
copying at least a portion of said digital file	See "Copying at least a portion of said digital file" ('193.1)
transferring at least a portion of said digital file to a second device	**Patent Specifications** '193 patent at 38:4-9 '193 patent at 65:24-38 '193 patent at 68:51-61 '193 patent at 72:1-9 '193 patent at 162:10-15 '193 patent at 167:41-43 '193 patent at 226:11-16 '193 patent at 237:34-47 '193 patent at 252:51-58 '193 patent at 324:8-37 '193 patent at 325:32-40 See "Transferring at least a portion of said digital file to a second device" (193.1); and "Storing information associated with said digital file in a secure database stored on said first device, said information including at least one control" (193.15)
storing said digital file	See "Storing said digital file" ('193.1)
'193:15	
receiving a digital file	**Patent Specifications** '193 patent at 52:66-53:8 '193 patent at 55:39-56 '193 patent at 60:37-48 '193 patent at 102:41-61 '193 patent at 133:39-134:23 '193 patent at 282:29-61 '193 patent at 316:16-317:19 See "Receiving a digital file" (193.11) **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 1508.
an authentication step comprising:	**Patent Specifications** '193 patent at 42:8-20 '193 patent at 47:49-57 '193 patent at 81:4-11 '193 patent at 123:24-62 '193 patent at 203:58-67 '193 patent at 212:66-213:36

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 230:22-27 '193 patent at 278:9-25 '193 patent at 279:41-60
accessing at least one identifier associated with a first device or with a user of said first device	**Patent Specifications** '193 patent at 25:31-38 '193 patent at 42:8-20 '193 patent at 47:49-57 '193 patent at 81:4-11 '193 patent at 123:23-62 '193 patent at 203:58-67 '193 patent at 212:65-213:36 '193 patent at 230:22-27 '193 patent at 278:9-25 '193 patent at 279:41-60 See Identifier
determining whether said identifier is associated with a device and/or user authorized to store said digital file	**Patent Specifications** '193 patent at 42:8-20 '193 patent at 47:49-57 '193 patent at 81:4-12 '193 patent at 123:24-62 '193 patent at 192:3-57 '193 patent at 203:58-67 '193 patent at 212:65-213:36 '193 patent at 230:22-27 '193 patent at 278:9-25 '193 patent at 279:42-60
storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized	**Patent Specifications** '193 patent at 42:8-20 '193 patent at 47:49-57 '193 patent at 81:4-12 '193 patent at 123:24-62 '193 patent at 192:3-57 '193 patent at 203:58-67 '193 patent at 212:65-213:36 '193 patent at 230:22-27 '193 patent at 278:9-25 '193 patent at 279:42-60
storing information associated with said digital file in a secure database stored on said first device, said information including at least one control	**Patent Specifications** '193 patent at 19:15-32 '193 patent at 22:20-25 '193 patent at 126:15-37 '193 patent at 153:50-67 '193 patent at 156:53-58 '193 patent at 292:19-47
determining whether said digital file may be copied and stored on a second device based on said at least one control	See "Determining whether said digital file may be copied and stored on a second device based on at least said copy control" ('193.1) and "Storing information associated with said digital file in a secure database stored on said first device, said information including at least one control" (193.15).

Claim Term / Phrase	InterTrust Evidence
if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,	**Patent Specification** '193 patent at 48:28-34 '193 patent at 102:26-40 '193 patent at 263:46-264:49 '193 patent at 265:9-38 '193 patent at 279:42-60 '193 patent at 316:16-317:19 See "If said first control allows at least a portion of said digital file to be copied and stored on a second device" ('193.11); "If said copy control allows at least a portion of said digital file to be copied and stored on a second device" (193.1); and "storing information associated with said digital file in a secure database stored on said first device, said information including at least one control" (193.15).
copying at least a portion of said digital file	See "Copying at least a portion of said digital file" ('193.1) and "Storing information associated with said digital file in a secure database stored on said first device, said information including at least one control" (193.15).
transferring at least a portion of said digital file to a second device	**Patent Specifications** '193 patent at 38:4-9 '193 patent at 65:24-38 '193 patent at 68:51-61 '193 patent at 72:1-9 '193 patent at 162:10-15 '193 patent at 167:41-43 '193 patent at 226:11-16 '193 patent at 237:34-47 '193 patent at 252:51-58 '193 patent at 324:8-37 '193 patent at 325:32-40 See "Transferring at least a portion of said digital file to a second device" (193.1); and "Storing information associated with said digital file in a secure database stored on said first device, said information including at least one control" (193.15).
storing said digital file	See "Storing said digital file" ('193.1).
'193:19	
receiving a digital file at a first device	**Patent Specifications** '193 patent at 52:66-53:8 '193 patent at 55:39-56 '193 patent at 60:37-48 '193 patent at 102:41-61 '193 patent at 133:39-134:23 '193 patent at 282:29-61 '193 patent at 316:16-317:19 See "Receiving a digital file" (193.11) **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 1508.
establishing communication between said first device and a clearinghouse located at a location remote from said first device	**Patent Specifications** '193 patent at 1:46-52 '193 patent at 1:60-63 '193 patent at 3:25-29

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 9:13-17
	'193 patent at 12:5-39
	'193 patent at 12:47-13:6
	'193 patent at 13:54-14:28
	'193 patent at 14:31-48
	'193 patent at 16:25-40
	'193 patent at 17:46-56
	'193 patent at 18:10-14
	'193 patent at 18:60-64
	'193 patent at 22:1-14
	'193 patent at 21:52-53; 23:51-24:14; and 24:57-25:30
	'193 patent at 38:43-55
	'193 patent at 45:19-26
	'193 patent at 45:39-45
	'193 patent at 46:4-8
	'193 patent at 52:66-53:8
	'193 patent at 53:13-22
	'193 patent at 53:33-37
	'193 patent at 53:45-59
	'193 patent at 54:51-58
	'193 patent at 55:21-56:24
	'193 patent at 57:33-39
	'193 patent at 58:59-64
	'193 patent at 59:39-42
	'193 patent at 60:37-48
	'193 patent at 62:27-42
	'193 patent at 63:32-39
	'193 patent at 64:49-51
	'193 patent at 65:9-14
	'193 patent at 67:31-52
	'193 patent at 68:65-69:12
	'193 patent at 74:51-53
	'193 patent at 75:23-28
	'193 patent at 75:65-76:32
	'193 patent at 81:26-32
	'193 patent at 83:53-63
	'193 patent at 90:1-28
	'193 patent at 90:39-46
	'193 patent at 91:26-51
	'193 patent at 96:1-7
	'193 patent at 96:12-26
	'193 patent at 98:66-99:3
	'193 patent at 99:28-35
	'193 patent at 101:54-102:52
	'193 patent at 104:29-37
	'193 patent at 105:25-39
	'193 patent at 115:13-21
	'193 patent at 115:25-29
	'193 patent at 123:51-55
	'193 patent at 131:45-52
	'193 patent at 135:16-24
	'193 patent at 135:31-42
	'193 patent at 153:53-156:47
	'193 patent at 160:65-162:65
	'193 patent at 170:42-172:13
	'193 patent at 172:61-177:53
	'193 patent at 178:49-179:55

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 214:59-67 '193 patent at 218:33-220:19 '193 patent at 220:53-67 '193 patent at 222:4-11 '193 patent at 225:22-226:36 '193 patent at 227:25-45 '193 patent at 231:32-59 '193 patent at 233:25-47 '193 patent at 234:36-43 '193 patent at 234:64-235:1 '193 patent at 235:13-38 '193 patent at 243:51-244:48 '193 patent at 254:30-34 '193 patent at 254:59-65 '193 patent at 264:26-49 '193 patent at 266:51-267:45 '193 patent at 273:42-53 '193 patent at 277:9-17 '193 patent at 279:42-53 '193 patent at 282:11-28 '193 patent at 282:45-61 '193 patent at 283:24-28 '193 patent at 283:56-284:43 '193 patent at 288:43-60 '193 patent at 289:14-27 '193 patent at 290:30-62 '193 patent at 292:19-47 '193 patent at 313:33-41 '193 patent at 313:58-67 '193 patent at 315:24-28 '193 patent at 316:1-6 '193 patent at 316:16-317:19 '193 patent, Figs. 1, 1A, 2, 2A, 3, 7, 8, 9, 9A, 10, 12, 13, 16, 19, 20, 21, 27, 28, 30, 31, 35, 36, 37, 38, 41a, 41b, 41c, 41d, 67, 69, 69A, 70, 71, 74, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, and 87
using said authorization information to gain access to or make at least one use of said first digital file	**Patent Specifications** '193 patent at 128:66-129:26 '193 patent at 148:50-149:7 '193 patent at 151:64-152:9 '193 patent at 215:24-32
receiving a first control from said clearinghouse at said first device	**Patent Specifications** '193 patent at 1:46-52 '193 patent at 1:60-2:3 '193 patent at 3:26-29 '193 patent at 9:13-16 '193 patent at 12:5-9 '193 patent at 12:47-13:6 '193 patent at 13:54-14:28 '193 patent at 14:31-48 '193 patent at 16:25-40 '193 patent at 17:46-56 '193 patent at 18:10-14 '193 patent at 18:60-64

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 22:1-14
	'193 patent at 21:52-53; 23:51-24:14; and 24:57-25:30
	'193 patent at 38:43-55
	'193 patent at 45:19-27
	'193 patent at 45:39-45
	'193 patent at 46:4-8
	'193 patent at 52:66-53:8
	'193 patent at 53:12-22
	'193 patent at 53:33-37
	'193 patent at 53:45-59
	'193 patent at 54:51-58
	'193 patent at 55:21-56:24
	'193 patent at 57:33-39
	'193 patent at 58:59-64
	'193 patent at 59:39-42
	'193 patent at 60:37-48
	'193 patent at 62:27-42
	'193 patent at 63:32-39
	'193 patent at 64:48-51
	'193 patent at 65:8-14
	'193 patent at 67:31-52
	'193 patent at 68:65-69:12
	'193 patent at 74:51-53
	'193 patent at 75:23-28
	'193 patent at 75:65-76:32
	'193 patent at 81:26-32
	'193 patent at 83:53-63
	'193 patent at 90:1-28
	'193 patent at 90:38-46
	'193 patent at 91:26-51
	'193 patent at 96:1-7
	'193 patent at 96:12-24
	'193 patent at 98:66-99:3
	'193 patent at 99:28-35
	'193 patent at 101:54-102:51
	'193 patent at 104:29-37
	'193 patent at 105:23-39
	'193 patent at 115:13-21
	'193 patent at 115:25-29
	'193 patent at 123:51-55
	'193 patent at 131:45-52
	'193 patent at 135:16-24
	'193 patent at 135:31-42
	'193 patent at 153:53-156:47
	'193 patent at 160:65-162:65
	'193 patent at 170:42-172:13
	'193 patent at 172:61-177:53
	'193 patent at 178:49-179:55
	'193 patent at 214:57-67
	'193 patent at 218:31-220:19
	'193 patent at 220:53-67
	'193 patent at 222:4-11
	'193 patent at 225:22-226:26
	'193 patent at 227:25-45
	'193 patent at 231:32-59
	'193 patent at 233:25-47
	'193 patent at 234:36-43

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 234:64-235:1 '193 patent at 235:13-38 '193 patent at 243:51-244:48 '193 patent at 254:30-34 '193 patent at 254:59-65 '193 patent at 264:29-49 '193 patent at 266:51-267:45 '193 patent at 273:42-53 '193 patent at 277:9-18 '193 patent at 279:42-53 '193 patent at 282:11-28 '193 patent at 282:45-61 '193 patent at 283:23-28 '193 patent at 283:56-284:42 '193 patent at 288:43-60 '193 patent at 289:14-27 '193 patent at 290:30-62 '193 patent at 292:19-47 '193 patent at 313:33-41 '193 patent at 313:58-67 '193 patent at 315:24-28 '193 patent at 316:1-6 '193 patent at 316:16-317:19 '193 patent, Figs. 1, 1A, 2, 2A, 3, 7, 8, 9, 9A, 10, 12, 13, 16, 19, 20, 21, 27, 28, 30, 31, 35, 36, 37, 38, 41a, 41b, 41c, 41d, 67, 69, 69A, 70, 71, 74, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, and 87 See "Receiving a digital file" (193.11).
storing said first digital file in a memory of said first device	See "Storing said digital file" ('193.1)
using said first control to determine whether said first digital file may be copied and stored on a second device	See "Determining whether said digital file may be copied and stored on a second device based on at least said copy control" ('193.1).
if said first control allows at least a portion of said first digital file to be copied and stored on a second device	**Patent Specifications** '193 patent at 48:28-35 '193 patent at 102:26-40 '193 patent at 263:46-264:57 '193 patent at 265:9-38 '193 patent at 279:42-60 '193 patent at 316:16-317:19 See "If said first control allows at least a portion of said digital file to be copied and stored on a second device" ('193.11).
copying at least a portion of said first digital file	See "Copying at least a portion of said digital file" ('193.1).
transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output	**Patent Specifications** '193 patent at 38:4-9 '193 patent at 65:24-38 '193 patent at 68:51-61 '193 patent at 72:1-9 '193 patent at 162:10-15 '193 patent at 167:41-43

48

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 226:11-16 '193 patent at 237:34-47 '193 patent at 252:51-58 '193 patent at 324:8-37 '193 patent at 325:32-40 See "Transferring at least a portion of said digital file to a second device" (193.1); and "Storing information associated with said digital file in a secure database stored on said first device, said information including at least one control" (193.15)
storing said first digital file portion	See "Storing said digital file" ('193.1)
'683:2	
the first secure container having been received from a second apparatus	**Patent Specifications** '683 patent at 15:56-16:4 '193 patent at 102:41-51
an aspect of access to or use of	**Patent Specifications** '683 patent at 24:33-39 '683 patent at 25:62-26:10 '193 patent at 15:46-50 '193 patent at 58:38-46 '193 patent at 159:23-26 '193 patent at 128:42-45
the first secure container rule having been received from a third apparatus different from said second apparatus	**Patent Specifications** '683 patent at 24:33-39 '683 patent at 25:62-67 '193 patent at 15:46-50 '193 patent at 54:24-38 '193 patent at 58:38-46 '193 patent at 128:42-45 '193 patent at 159:23-26 See "First secure container having been received from a second apparatus" (683.2).
hardware or software used for receiving and opening secure containers	**Patent Specifications** '683 patent at 5:30-38 '683 patent at 6:52-56 '683 patent at 8:50-52 '683 patent at 10:12-15 '683 patent at 10:27-35 '683 patent at 10:55-11:14 '683 patent at 11:40-52 '683 patent at 11:65-56 '683 patent at 11:59-64 '683 patent at 12:27-51 '683 patent at 13:3-6 '683 patent at 13:15-17 '683 patent at 13:43-47 '683 patent at 14:10-14 '683 patent at 14:18-27

Claim Term / Phrase	InterTrust Evidence
	'683 patent at 14:58
	'683 patent at 14:64-65
	'683 patent at 15:35-45
	'683 patent at 15:56-16:4
	'683 patent at 16:25-28
	'683 patent at 16:58-20:66
	'683 patent at 24:46-25:26
	'683 patent at 29:50-30:16
	'683 patent at 30:30-35:43
	'683 patent at 36:1-37:42
	'683 patent at 38:56-39:39
	'683 patent at 39:66-43:20
	'683 patent at 47:34-42
	'683 patent at 49:31-39
	'683 patent at 61:7-11
	'683 patent at 62:8-62
	'683 patent, Figs. 7, 8, 9, 9A, 9B, 10, 12, 13, 35, 36
	'193 patent at 1:46-55
	'193 patent at 1:60-63
	'193 patent at 3:26-29
	'193 patent at 9:13-17
	'193 patent at 12:5-39
	'193 patent at 12:47-13:6
	'193 patent at 13:54-14:28
	'193 patent at 14:31-48
	'193 patent at 16:25-40
	'193 patent at 17:46-56
	'193 patent at 18:10-14
	'193 patent at 18:60-64
	'193 patent at 22:1-14
	'193 patent at 21:52-53; 23:51-24:14; 24:57-25:30
	'193 patent at 38:46-55
	'193 patent at 45:19-27
	'193 patent at 45:39-45
	'193 patent at 46:4-8
	'193 patent at 52:66-53:8
	'193 patent at 53:13-22
	'193 patent at 53:33-37
	'193 patent at 53:45-59
	'193 patent at 54:51-58
	'193 patent at 55:21-56:24
	'193 patent at 57:33-39
	'193 patent at 58:59-64
	'193 patent at 59:39-42
	'193 patent at 60:37-48
	'193 patent at 62:27-42
	'193 patent at 63:32-39
	'193 patent at 64:48-51
	'193 patent at 65:8-14
	'193 patent at 67:31-52
	'193 patent at 68:65-69:12
	'193 patent at 74:51-53
	'193 patent at 75:23-28
	'193 patent at 75:65-76:32
	'193 patent at 81:26-32
	'193 patent at 83:52-63

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 90:1-28
	'193 patent at 90:38-46
	'193 patent at 91:26-51
	'193 patent at 96:1-7
	'193 patent at 96:12-24
	'193 patent at 98:66-99:3
	'193 patent at 99:28-35
	'193 patent at 101:54-102:51
	'193 patent at 104:29-37
	'193 patent at 105:23-39
	'193 patent at 115:13-21
	'193 patent at 115:25-29
	'193 patent at 123:51-55
	'193 patent at 135:31-42
	'193 patent at 153:53-156:47
	'193 patent at 161:7-162:65
	'193 patent at 170:42-172:13
	'193 patent at 172:61-177:53
	'193 patent at 178:49-179:55
	'193 patent at 214:57-67
	'193 patent at 218:31-219:19
	'193 patent at 220:53-67
	'193 patent at 222:4-11
	'193 patent at 225:22-226:36
	'193 patent at 227:25-45
	'193 patent at 231:32-59
	'193 patent at 233:25-47
	'193 patent at 234:36-43
	'193 patent at 234:64-235:1
	'193 patent at 235:14-38
	'193 patent at 243:51-244:48
	'193 patent at 254:30-34
	'193 patent at 254:59-65
	'193 patent at 264:29-49
	'193 patent at 266:51-267:45
	'193 patent at 273:42-53
	'193 patent at 277:9-17
	'193 patent at 279:42-53
	'193 patent at 282:11-28
	'193 patent at 282:45-61
	'193 patent at 283:23-28
	'193 patent at 283:56-284:42
	'193 patent at 288:43-60
	'193 patent at 289:14-27
	'193 patent at 290:30-62
	'193 patent at 313:33-41
	'193 patent at 313:58-67
	'193 patent at 315:25-29
	'193 patent at 316:1-6
	'193 patent at 316:62-65
	'193 patent, Figs. 1, 1A, 2, 2A, 3, 7, 8, 9, 9A, 10, 12, 13, 16, 19, 20, 21, 27, 28, 30, 31, 35, 36, 37, 38, 41a, 41b, 41c, 41d, 67, 69, 69A, 70, 71, 74, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, and 87
	File Histories
	'683 File History, 11/12/99 Office Action, pp. 4-5 (citing USP 5,412,717); see also USP 5,412,717 at 4:45-62; 7:49-56; 8:7-24; and 9:64-66.

Claim Term / Phrase	InterTrust Evidence
	See Protected Processing Environment and Host Processing Environment
said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers	**Patent Specifications** '683 patent at 15:56-16:4 '683 patent at 25:62-26:10 '193 patent at 19:15-32 '193 patent at 22:20-25 '193 patent at 292:27-37
protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus	See Protected Processing Environment
hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container	**Patent Specifications** '683 patent at 8:38-46 '683 patent at 11:40-52 '683 patent at 11:55-56 '683 patent at 11:59-64 '683 patent at 13:46-47 '683 patent at 14:58 '683 patent at 16:25-28 '683 patent at 16:58-62 '683 patent at 20:13-23 '683 patent at 24:26-33 '683 patent at 25:62-26:10 '683 patent at 29:50-30:3 '683 patent at 30:40-65 '683 patent at 31:28-55 '683 patent at 32:7-36 '683 patent at 32:59-33:37 '683 patent at 34:5-13 '683 patent at 35:44-67 '683 patent at 36:13-40 '683 patent at 37:14-42 '193 patent at 19:63-20:7 '193 patent at 54:39-50 '193 patent at 55:33-56 '193 patent at 149:24-45 '193 patent at 242:54-61 '193 patent at 242:64-243:9 '193 patent at 243:59-62 '193 patent at 253:9-63 **File Histories** '683 File History, 11/12/99 Office Action, pp. 4-5 (citing USP 5,412,717 at 10:8-39 and 17:40-61). See Protected Processing Environment and Host Processing Environment
hardware or software used for	**Patent Specifications**

Claim Term / Phrase	InterTrust Evidence
transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	'683 patent at 5:30-40 '683 patent at 6:52-56 '683 patent at 8:50-52 '683 patent at 10:12-15 '683 patent at 10:27-35 '683 patent at 10:55-11:14 '683 patent at 11:40-51 '683 patent at 11:55-56 '683 patent at 11:59-64 '683 patent at 12:27-51 '683 patent at 13:3-6 '683 patent at 13:14-16 '683 patent at 13:43-47 '683 patent at 14:11-22 '683 patent at 14:58-60 '683 patent at 14:64-65 '683 patent at 15:16-17 '683 patent at 15:26-27 '683 patent at 15:35-45 '683 patent at 15:56-16:4 '683 patent at 16:25-28 '683 patent at 16:58-20:51 '683 patent at 24:46-25:26 '683 patent at 29:50-30:16 '683 patent at 30:30-35:43 '683 patent at 36:1-37:42 '683 patent at 38:56-39:39 '683 patent at 39:65-43:20 '683 patent at 47:34-42 '683 patent at 49:31-39 '683 patent at 61:7-11 '683 patent at 62:9-62 '683 patent, Figs. 7, 8, 9, 9A, 9B, 10, 12, 13, 35, 36 '193 patent at 1:46-52 '193 patent at 1:60-63 '193 patent at 3:26-29 '193 patent at 9:13-17 '193 patent at 12:5-39 '193 patent at 12:47-13:6 '193 patent at 13:54-14:28 '193 patent at 14:31-48 '193 patent at 16:25-40 '193 patent at 17:46-56 '193 patent at 18:10-14 '193 patent at 18:60-64 '193 patent at 22:1-14 '193 patent at 21:52-53; 23:51-24:14; 24:57-25:30 '193 patent at 38:43-55 '193 patent at 45:19-27 '193 patent at 45:39-45 '193 patent at 46:4-8 '193 patent at 52:66-53:8 '193 patent at 53:13-22 '193 patent at 53:33-37 '193 patent at 53:45-59 '193 patent at 54:51-58

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 55:21-56:24
	'193 patent at 57:33-39
	'193 patent at 58:59-64
	'193 patent at 59:39-41
	'193 patent at 60:37-48
	'193 patent at 62:27-42
	'193 patent at 63:32-39
	'193 patent at 64:48-51
	'193 patent at 65:8-14
	'193 patent at 67:31-52
	'193 patent at 68:65-69:12
	'193 patent at 74:51-53
	'193 patent at 75:23-28
	'193 patent at 75:65-76:32
	'193 patent at 81:26-32
	'193 patent at 83:53-63
	'193 patent at 90:1-28
	'193 patent at 90:39-46
	'193 patent at 91:26-51
	'193 patent at 96:1-7
	'193 patent at 96:12-20
	'193 patent at 98:66-99:3
	'193 patent at 99:28-35
	'193 patent at 101:54-102:51
	'193 patent at 104:29-37
	'193 patent at 105:23-39
	'193 patent at 115:13-21
	'193 patent at 115:25-29
	'193 patent at 123:51-55
	'193 patent at 135:31-42
	'193 patent at 153:53-156:47
	'193 patent at 161:7-162:65
	'193 patent at 170:42-172:13
	'193 patent at 172:61-177:53
	'193 patent at 178:49-179:55
	'193 patent at 214:57-67
	'193 patent at 218:31-220:19
	'193 patent at 220:53-67
	'193 patent at 222:4-11
	'193 patent at 225:22-226:36
	'193 patent at 227:25-45
	'193 patent at 231:32-59
	'193 patent at 233:25-47
	'193 patent at 234:36-43
	'193 patent at 234:64-235:1
	'193 patent at 235:14-38
	'193 patent at 243:51-255:48
	'193 patent at 254:30-34
	'193 patent at 255:59-65
	'193 patent at 264:29-49
	'193 patent at 266:51-267:45
	'193 patent at 273:42-53
	'193 patent at 277:10-17
	'193 patent at 279:42-53
	'193 patent at 282:11-28
	'193 patent at 282:45-61
	'193 patent at 283:23-28

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 283:56-284:42 '193 patent at 288:43-60 '193 patent at 289:14-27 '193 patent at 290:30-62 '193 patent at 313:33-41 '193 patent at 313:58-67 '193 patent at 315:25-29 '193 patent at 316:1-6 '193 patent at 316:62-65 '193 patent, Figs. 1, 1A, 2, 2A, 3, 7, 8, 9, 9A, 10, 12, 13, 16, 19, 20, 21, 27, 28, 30, 31, 35, 36, 37, 38, 41a, 41b, 41c, 41d, 67, 69, 69A, 70, 71, 74, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, and 87 **File Histories** '683 File History, 11/12/99 Office Action, pp. 4-5 (citing USP 5,412,717); see also USP 5,412,717 at 1:18-24; 4:58-69. See Protected Processing Environment and Host Processing Environment
'721:1	
digitally signing a first load module with a first digital signature designating the first load module for use by a first device class	**Patent Specifications** '721 patent at 4:61-5:5 '721 patent at 6:16-62 '721 patent at 7:66-8:6 '721 patent at 16:37-17:23 '721 patent at 18:19-39 '721 patent at 19:11-32 '721 patent at 20:1-4
digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class	**Patent Specifications** '721 patent at 4:61-5:9 '721 patent at 6:16-64 '721 patent at 7:62-8:6 '721 patent at 16:37-17:23 '721 patent at 17:41-18:2 '721 patent at 18:19-20:4
distributing the first load module for use by at least one device in the first device class	**Patent Specifications** '721 patent at 4:61-5:5 '721 patent at 6:16-62 '721 patent at 7:66-8:6 '721 patent at 16:37-17:23 '721 patent at 18:3-38 '721 patent at 19:11-32 '721 patent at 19:51-67 '721 patent at 20:1-4 '721 patent at 20:58-21:7
distributing the second load module for use by at least one device in the second device class	**Patent Specifications** '721 patent at 4:61-5:5 '721 patent at 6:16-62

Claim Term / Phrase	InterTrust Evidence
device in the second device class	'721 patent at 7:66-8:6 '721 patent at 16:37-17:23 '721 patent at 18:3-38 '721 patent at 19:11-32 '721 patent at 19:51-67 '721 patent at 20:1-4 '721 patent at 20:58-21:7
'721:34	
arrangement within the first tamper resistant barrier	**Patent Specifications** '721 patent at 4:61-5:9 '721 patent at 6:5-7:7 '721 patent at 7:62-8:6 '721 patent at 16:37-17:23 '721 patent at 17:41-18:2 '721 patent at 18:19-39 '721 patent at 19:11-20:25
prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level	**Patent Specifications** '721 patent at 4:61-5:9 '721 patent at 6:5-7:7 '721 patent at 7:62-8:6 '721 Patent at 16:37-17:23 '721 patent at 17:41-18:2 '721 Patent at 18:19-39 '721 patent at 19:11-20:25
'861:58	
creating a first secure container	**Patent Specifications** '861 patent at 3:3-4 '861 patent at 3:39-43 '861 patent at 6:29-32 '861 patent at 10:7-10 '861 patent at 11:48-58 '861 patent at 16:32-35 See Secure Container
including or addressing . . . organization information . . . desired organization of a content section. . . and metadata information at least in part specifying at least one step required or desired in creation of said first secure container	**Patent Specifications** '861 patent at 5:57-6:7 '861 patent at 10:38-53 '861 patent at 14:14-29 '861 patent at 15:21-31 '861 patent at 17:49-53
at least in part determine specific information required to be included in said first secure container contents	**Patent Specifications** '861 patent at 10:49-61 '861 patent at 15:21-31 '861 patent at 28:26-28 '193 patent at 69:66-70:1 '193 patent at 71:19-20 '193 patent at 230:30-34

Claim Term / Phrase	InterTrust Evidence
rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents	**Patent Specifications** '861 patent at 15:21-31 '861 patent at 17:49-53
'891:1	
resource processed in a secure operating environment at a first appliance	**Patent Specifications** '193 patent at 83:44-48 See Protected Processing Environment
securely receiving a first entity's control at said first appliance	**Patent Specifications** '193 patent at 55:52-54 '193 patent at 57:27-36 '193 patent at 60:37-48 '193 patent at 62:32-39 '193 patent at 67:21-52 '193 patent at 68:65-69:12 '193 patent at 75:65-76:1 '193 patent at 76:10-32 '193 patent at 77:30-44 '193 patent at 81:26-32 '193 patent at 83:53-84:7 '193 patent at 91:38-51 '193 patent at 96:1-6 '193 patent at 96:12-17 '193 patent at 101:54-102:25 '193 patent at 102:41-51 '193 patent at 104:29-37 '193 patent at 118:64-119:43 '193 patent at 123:22-28 '193 patent at 123:51-56 '193 patent at 155:51-156:2 '193 patent at 160:66-161:51 '193 patent at 162:39-163:35 '193 patent at 200:66-201:42 '193 patent at 211:39-212:10 '193 patent at 214:59-67 '193 patent at 218:31-220:19 '193 patent at 225:50-226:36 '193 patent at 227:25-228:30 '193 patent at 233:25-35 '193 patent at 282:56-61 '193 patent at 283:61-65 '193 patent at 290:46-62 '891 patent at 322:56-63 See "Securely Receiving"; and "Receiving a first control from said clearinghouse at said first device" (193.19)
securely receiving a second entity's control at said first appliance	See "Securely receiving a first entity's control at said first appliance" (891.1)
securely processing a data item at	See "Resource processed in a secure operating environment at a first appliance"

Claim Term / Phrase	InterTrust Evidence
said first appliance, using at least one resource	(891.1); and "Securely Processing."
securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item ·	**Patent Specifications** '891 patent at 322:16-18 See "Resource processed in a secure operating environment at a first appliance" (891.1); and "Securely Applying"
'900:155	
first host processing environment comprising	See Host Processing Environment
designed to be loaded into said main memory and executed by said central processing unit	**Patent Specifications** '900 patent at 82:12-23
said tamper resistant software comprising: . . . one or more storage locations storing said information	**Patent Specifications** '900 patent at 239:50-53
derives information from one or more aspects of said host processing environment,	**Patent Specifications** '900 patent at 239:4-42
one or more storage locations storing said information	**Patent Specifications** '900 patent at 239:4-21 '900 patent at 239:50-60 '900 patent, Fig. 69C '900 patent, Fig. 69G
information previously stored in said one or more storage locations	**Patent Specifications** '900 patent at 239:15-55 '900 patent at 240:31-34
generates an indication based on the result of said comparison	**Patent Specifications** '900 patent at 239:56-64 '900 patent at 243:32-41
programming which takes one or more actions based on the state of said indication	**Patent Specifications** '900 patent at 239:56-64 '900 patent at 242:52-67 '900 patent at 243:32-41 '900 patent at 243:65-244:2 '900 patent at 244:33-39 '900 patent at 247:50-57
at least temporarily halting further processing	**Patent Specifications** '900 patent at 239:56-64 '900 patent at 242:52-67 '900 patent at 243:32-41 '900 patent at 243:65-244:2 '900 patent at 244:33-39 '900 patent at 247:50-57

Claim Term / Phrase	InterTrust Evidence
'912:8	
identifying at least one aspect of an execution space required for use and/or execution of the load module	**Patent Specifications** '193 patent at 140:15-46
said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security	**Patent Specifications** '193 patent at 140:15-46 '912 patent at 327:59-61 '912 patent at 327:64-66
checking said record for validity prior to performing said executing step	**Patent Specifications** '193 patent at 112:46-113:2 **File Histories** '912 File History, 9/22/98 Office Action, pp. 2-3.
'912.35	
received in a secure container	**Patent Specifications** '193 patent at 58:48-58
said component assembly allowing access to or use of specified information	**Patent Specifications** '193 patent at 69:66-70:1 '193 patent at 71:19-20 '193 patent at 83:53-84:16 '193 patent at 159:61-160:8 '193 patent at 230:30-34 **Extrinsic Sources** The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992) ("information") '193 patent at 69:66-70:1 '193 patent at 71:19-20 ' 193 patent at 230:30-34
said first component assembly specified by said first record	See "Said component assembly allowing access to or use of specified information" (912.35)
	Evidence Relevant to Numerous Disputed Claim Terms and Phrases
Refreshing a budget	**Patent Specifications** '193 patent at 131:10-13 '193 patent at 162:39-65 '193 patent at 173:21-174:14
Absolute protection	**Patent Specifications** '193 patent at 16:25-28 '193 patent at 35:59-63 '193 patent at 38:4-12 '193 patent at 49:59-62 '193 patent at 80:65-81:8

Claim Term / Phrase	InterTrust Evidence
	'193 patent at 199:38-46 '193 patent at 221:2-6 '193 patent at 222:49-53 '193 patent at 223:4-10 '721 patent at 21:9-24 '721 patent at 24:48-56 **Citations from Sources Designated by Microsoft under PLR 4-2(b)** Landwehr, Formal Models for Computer Security, ACM Computer Surveys (Sept. 3, 1981), p. 253. Computer Security Handbook, 2d ed. (Macmillan, 1988), pp. 75, 201, 218, 292-93 Hoffman, Modern Methods for Computer Security and Privacy (Prentice-Hall, 1977), p. 170. Garfinkel et al., Practical Unix Security (O'Reilly & Associates, 1991), pp. 12-13. Neumann, Computer Related Risks (ACM Press, 1995), p. 2.
Alternative control structures	**Patent Specifications** '193 patent at 28:29-37 '193 patent at 30:42-31:7 '193 patent at 31:29-56 '193 patent at 48:15-35 '193 patent at 306:30-65 '193 patent at 308:29-42 '193 patent at 308:48-65 '193 patent at 312:11-31
Digital file versus a copy	**Patent Specifications** '193 patent at 162:10-15 '193 patent at 226:11-16 '193 patent at 278:11-21 '193 patent at 316:16-37 '193 patent at 324:8-37 '193 patent at 325:32-40
Host Processing Environments and Secure Processing Environments	**Patent Specifications** '193 patent at 13:7-14 '193 patent at 79:24-80:21 '193 patent at 80:65-81:8 '193 patent at 278:46-65 '683 patent at 29:51-30:3 '721 patent at 3:16-21

Exhibit D

EXHIBIT D

PLR 4-3(b) –Microsoft's Listing of Intrinsic and Extrinsic Evidence

Each claim phrase incorporates the Intrinsic and Extrinsic support of the individual terms within it.

Claim Term	MS Construction
access, accessed, access to, accessing 193.15, 193.19, 912.8, 912.35, 861.58, 683.2, 721.34	**Intrinsic:** - "These rights govern use of the VDE object 300 by that user or user group. For instance, the user may have an "access" right, and an "extraction" right, but not a "copy" right." ('193 159:32)[1] - ('193 82:27-45); ('193 109:53-57); ('193 118:17-31); (193 139:60-140:6); ('193 148:55-58); ('193 183:12-29); ('193 188:59-67); ('193 192:2-24) **Extrinsic:**[2] Access (n): 2. The use of an access method. 3. The manner in which files or data sets are referred to by the computer. 5. In computer security, a specific type of interaction between a subject and an object that results in the flow of information from one to the other. (IBM)[3] Access (n.): 1. In access control, a specific type of interaction between a subject and an object that results in the flow of information from on to the other 3. In computing, the manner in which files or data sets are referred to by a computer (Longley)[4] Access(ing) (v.): 1. To obtain the use of a computer resource. 4. To obtain data from or to put data in storage. (IBM)
addressing 861.58	**Intrinsic:** "Load modules 1100 in the preferred embodiment are modular and "code pure" so that individual load modules may be reenterable and reusable. In order for components 690 to be dynamically updatable, they may be individually addressable within a global public name space." ('193 86:49-53) **Extrinsic:** Addressing (v): 1. A character or group of characters that identifies a register, a particular part of storage, or some other data source or destination. 4. A name, label, or number identifying a location in storage, a device in a system or network, or any other data source. 5. In data communication, the unique code assigned to each device or workstation connected to a network.(IBM) Addressing (n.): 1. In computing, a character or group of characters that identifies a register, a particular part of storage, or some other data source or destination 2. In computing, to refer to a device or an item of data by its address. (Longley) Addressing (v): 1. In computing, the assignment of addresses to the instructions of a program 2. In communications, the means whereby the originator or control station selects the unit to which it is going to send a message (Longley)
allowing, allows 912.35, 193.1, 193.11, 193.15, 193.19	**Intrinsic:** - SN 08/780,545 ('912): 10/29/98 amendment to claim 211 (issued claim 35) "necessary in order to gain" to "allowing" - VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users." ('193 4:51-56)

---

[1] Citations to the '193 Patent are representative of citations to the text and drawings of the "Big Book" application also published in the '891, '900, and '912 Patents. Emphasis is added unless otherwise noted.
[2] Extrinsic evidence is cited herein without waiver of any kind, including relevance or probative value.
[3] "IBM" herein refers to IBM Dictionary of Computing, 10th ed., 1983.
[4] "Longley" herein refers to Longley, D., et al, Information Security: Dictionary of Concepts, Standards, and Terms, 1992

Claim Term	MS Construction
	- VDE is a secure system for regulating electronic conduct and commerce. Regulation is ensured by control information put in place by one or more parties. ('193 6:33-34)
	- VDE ensures that certain prerequisites necessary for a given transaction to occur are met. ('193 20:27-28)
	- ('193 309:10-16); ('193 15:41-46); ('193 17:22-28); ('193 303:67-304:1)
	Extrinsic:
	Least privilege: Each user and each program should operate using the fewest privileges possible. In this way, the damage from an inadvertent or malicious attack is minimized. (Pfleeger)[5]
arrangement 721.34	See also phrases of use in 721.34. Intrinsic: An important part of VDE provided by the present invention is the core secure transaction control arrangement, herein called an SPU (or SPUs), that typically must be present in each user's computer, other electronic appliance, or network. ('193 48:66)
aspect 900.155, 912.8, 861.58, 683.2	See also phrases of use in 900.155, 912.8, 861.58, 683.2. Extrinsic: Aspect: The qualification of a descriptor. (IBM)
associated with 912.8, 193.1, 193.11, 193.15, 683.2	Intrinsic: - "VDEF load modules, associated data, and methods form a body of information that for the purposes of the present invention are called "control information." VDEF control information may be specifically associated with one or more pieces of electronic content and/or it may be employed as a general component of the operating system capabilities of a VDE installation." ('193 18:36-42) - "As mentioned above, virtual distribution environment 100 "associates" content with corresponding "rules and controls," and prevents the content from being used or accessed unless a set of corresponding "rules and controls" is available." ('193 57:18-22) - "This "lookup" mechanism permits electronic appliance 600 to associate, in a secure way, VDE objects 300 with PERCs 808, methods 1000 and load modules 1100." ('193 153:35-38) - ('193 55:39-45); ('193 142:50-52); ('193 57:30-33); ('861 1:50-53) Extrinsic: Association: In the Open Systems Interconnection reference model, a cooperative relationship between two peer entities, supported by the exchange of protocol control information using the services of the next lower layer. (IBM)
authentication 193.15	Intrinsic: - A certification key pair may be used as part of a "certification" process for PPEs 650 and VDE electronic appliances 600. This certification process in the preferred embodiment may be used to permit a VDE electronic appliance to present one or more "certificates" authenticating that it (or its key) can be trusted. As described above, this "certification" process may be used by one PPE 650 to "certify" that it is an authentic VDE PPE, it has a certain level of security and capability set (e.g., it is hardware based rather than merely software based), etc. ('193 212:66-213:15) - "One of the functions SPU 500 may perform is to validate/authenticate VDE objects 300 and other items. Validation/authentication often involves comparing long data strings to determine whether they compare in a predetermined way." ('193 67:56-60)

---

[5] "Pfleeger" herein refers to Pfleeger, Security in Computing (1989).

Claim Term	MS Construction
	- ('683 17:20-27); ('683 52:56-60); ('193 112:46-61)
	Extrinsic:
	Authentication: 1. In computer security, verification of the identity of a user or the user's eligibility to access an object. 2. In computer security, verification that a message has not been altered or corrupted. 3. In computer security, a process used to verify the user of an information system or protected resources. 4. A process that checks the integrity of an entity. (IBM)
	Authentication: 1. In data security, the act of determining that a message has not been changed since leaving its point of origin. 4. In computer security, the act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information (Longley)
authorization information, authorized, not authorized 193.15, 193.19	Intrinsic: - See "allow." Several independent comparisons may be used to ensure there has been no unauthorized substitution. For example, the public and private copies of the element ID may be compared to ensure that they are the same, thereby preventing gross substitution of elements. In addition, a validation/correlation tag stored under the encrypted layer of the loadable element may be compared to make sure it matches one or more tags provided by a requesting process. This prevents unauthorized use of information. ('193 87:47-55) "using said authorization information to gain access to or make at least one use of said first digital file" ('193 Claim 19) Extrinsic: Authorization: 1 In computer security, the right granted to a user to communicate with or make use of a computer system. 2. An access right. 3. The process of granting a user either complete or restricted access to an object, resource, or function. (IBM) Authorization: (1) In access control, the granting to a user, a program, or a process the right of access. (2) In operations, the right given to a user to communicate with or make use of a computer system or stored data. 3. The privilege granted to an individual by a designated official to access information based upon the individual's clearance and need-to-know. (Longley) Authorization: "A system control feature that requires specific approval before the processing can take place." (Webster's New World Dictionary of Computer Terms, 4th ed., 1992)
budget control; budget 193.1	Intrinsic: - ""Budgets" 308 shown in FIG. 5B are a special type of "method" 1000 that may specify, among other things, limitations on usage of information content 304, and how usage will be paid for. Budgets 308 can specify, for example, how much of the total information content 304 can be used and/or copied. The methods 310 may prevent use of more than the amount specified by a specific budget." ('193 59:19-25) (See also Fig. 5B) - "For example, consider the case of a security budget. One form of a typical budget might limit the user to 10Mb of decrypted data per month." ('193 265:9-11) - "An example of the process steps used for the move of a budget record might look something like this: 1) Check the move budget (e.g., to determine the number of moves allowed) ('193 265:24-27) - "BUDGET method 408 may store budget information in a budget UDE" ('193 182:25-26) - "In the preferred embodiment, a "method" 1000 is a collection of basic instructions, and information related to basic instructions, that provides context, data, requirements and/or relationships for use in performing, and/or preparing a perform, basic instructions in relation to the operation of one or more electronic appliances 600." ('193 85:43-48; repeated essentially at '193 136:20-25) - BUDGET method 408 may result in a "budget remaining" field in a budget UDE being decremented

Claim Term	MS Construction
	by an amount specified by BILLING method 406. ('193 182:22-30) - ('193 58:27-34); ('193 187:48-50); ('193 235:39-42); ('193 143:63 - 144:14); ('193 265:44-51) **Extrinsic:** Budget: A budget is the control mechanism for a meterable feature. A budget provides an upper limit for the volume of a meterable feature that a user (client) may use. Budgets consist of two values: a ceiling limit on use and an increment value that is added to the associated meter when a meterable event occurs. Budgets may be stand-alone or cascaded. A stand-alone budget only increments the meters for itself, while a cascaded budget can increment many meters from a single meterable event. A budget consists of an identification sextet, a descriptive area that describes the budget (cascade budget tuple and other miscellaneous flags), and a series of budget tuples. Each budget tuple consists of a budget and the increment value. It should be noted that a budget may be specified in meterable events or in dollars, based on the type of meter the budget will be compared against. (VDE ROI Device v1.0a, 9 Feb 1994, IT00008582) Control: The determination of the time and order in which the parts of a data processing system and the devices that contain those parts perform the input, processing, storage, and output functions. (IBM) Budget Object: A governed element that defines the consumer's ability to provide payment using a specific payment type. ((ITG, 1997-1998, ML00012B)[6] Budget Object: *An InterTrust system object* that defines the consumer's ability to provide payment using a specific payment type. ((emphasis added) IT System Developers Kit, 1997, TD00298C) Budget: A control mechanism that limits operations on content based on billed amounts that can maintain a budget trail. A budget may be financially based (e.g., a number of dollars available for purchasing content use) or abstract (e.g. a total number of permitted usages). VTG, 3/7/95, IT00709617) Budget: *A fixed quantity of money, time, etc. against which the cost of operation is charged. Budget activities usually also involve reporting. ((ITG, 8/21/95, IT0032371) Control: Defines rules and consequences for operations on a Property Chunk. A Control may be implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node. ((ITG, 5/12/95, IT00028293) Control: A business rule that governs the use of content. ((ITG, 1997-1998, ML00012B) Control: A set of rules and consequences that apply to a governed element. The term control can apply to either a control program or a control set. ((ITG, 1997-2000, ML00012D) Control: *Control Element:* A data structure that giverns (sic) the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). *Control mechanism:* One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. * *Control object:* A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. *Control Parameter:* A data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself. ((ITG, 3/7/1995, IT00709618, see footnote 2)
can be 193.1	Intrinsic: VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content

---

[6] "(ITG" herein is a generic reference to several InterTrust glossaries that are further identified by Bates number or IT document number.

Claim Term	MS Construction
	users." ('193 4:51-56)
	- VDE is a secure system for regulating electronic conduct and commerce. Regulation is ensured by control information put in place by one or more parties. ('193 6:33-35)
	- It also employs a software object architecture for VDE content containers that carries protected content and may also carry both freely available information (e.g., summary, table of contents) and secured content control information which ensures the performance of control information. ('193 15:41-46)
	- Because of the breadth of issues resolved by the present invention, it can provide the emerging "electronic highway" with a single transaction/distribution control system that can, for a very broad range of commercial and data security models, ensure against unauthorized use of confidential and/or proprietary information and commercial electronic transactions. ('193 17:22-28)
	- VDE ensures that certain prerequisites necessary for a given transaction to occur are met. ('193 20:27-28)
	- "support "launchable" content, that is content that can be provided by a content provider to an end-user, who can then copy or pass along the content to other end-user parties without requiring the direct participation of a content provider to register and/or otherwise initialize the content for use." ('193 24:57-62)
	- "For example, budget process 408 may limit the number of times content may be accessed or copied, or it may limit the number of pages or other amount of content that can be used based on, for example, the number of dollars available in a credit account." ('193 58:28-32)
	- "Budgets 308 can specify, for example, how much of the total information content 304 can be used and/or copied. The methods 310 may prevent use of more than the amount specified by a specific budget." ('193 59:22-25)
	- "As an alternative example, a creator may allow moving of usage rights by a distributor to half a dozen subdistributors, each of whom can distribute 10,000 copies, but with no redistribution rights being allowed to be allocated to subdistributors' (redistributors') customers. ... Content providers and other contributors of control information have the ability through the use of permissions records and/or component assemblies to control rights other users are authorized to delegate in the permissions records they send to those users, so long as such right to control one, some, or all such rights of other users is either permitted or restricted (depending on the control information distribution model)." ('193 269:34-49)
	"In such systems, because document content can be freely copied and manipulated, it is not possible to determine where document content has gone, or where it came from." ('193 281:33-36)
capacity 683.2	Intrinsic: "Some items may be too large to store within container 302." ('193 58:54-55) ('193 243:23 – 244:48) Extrinsic: Capacity: See channel capacity, storage capacity.(IBM) Channel Capacity: The measure of the ability of a given channel subject to specific constraints to transmit messages from a specified message source expressed as either the maximum possible mean transinformation content per character or the maximum possible average transinformation rate, which can be achieved with an arbitrary small probability of errors by use of an appropriate code. (IBM) Storage capacity: The amount of data that can be contained in a storage device measured in binary characters, bytes, words, or other units. For registers, the term "register length" is used with the same meaning. Synonymous with storage size. (IBM)
clearinghouse	Intrinsic:

Claim Term	MS Construction
193.19	- "Distribution involves three types of entity. Creators usually are the source of distribution. They typically set the control structure "context" and can control the rights which are passed into a distribution network. Distributors are users who form a link between object (content) end users and object (content) creators. They can provide a two-way conduit for rights and audit data. Clearinghouses may provide independent financial services, such as credit and/or billing services, and can serve as distributors and/or creators. Through a permissions and budgeting process, these parties collectively can establish fine control over the type and extent of rights usage and/or auditing activities." ('193 267:34-45) - "Payment credit or currency may then be automatically communicated in protected (at least in part encrypted) form through telecommunication of a VDE container to an appropriate party such as a clearinghouse, provider of original property content or appliance, or an agent for such provider (other than a clearinghouse)." ('193 36:64-37:3) "if appropriate credit (e.g. an electronic clearinghouse account from a clearinghouse such as VISA or AT &T) is available" ('193 25:22-24) Extrinsic: Clearinghouse: *A facility that receives reports of content use and in turn reports payments and usage to content creators and distributors. (ITG, 8/21/95, IT00032372, TD00068B)
compares, comparison 900.155	Intrinsic: "ROS 602 also provides a tagging and sequencing scheme that may be used within the loadable component assemblies 690 to detect tampering by substitution. Each element comprising a component assembly 690 may be loaded into an SPU 500, decrypted using encrypt/decrypt engine 522, and then tested/compared to ensure that the proper element has been loaded. Several independent comparisons may be used to ensure there has been no unauthorized substitution. For example, the public and private copies of the element ID may be compared to ensure that they are the same, thereby preventing gross substitution of elements." ('193 87:41-51) Extrinsic: Compare: 1. To examine two items to discover their relative magnitudes, their relative positions in an order or in a sequence, or whether they are identical in given characteristics. 2. To examine two or more items for identity, similarity, equality, relative magnitude, or order in a sequence.(IBM) Comparison: The process of examining two or more items for identity, similarity, equality, relative magnitude, or for order in sequence. (IBM)
component assembly 912.8, 912.35	Intrinsic: - "Many such load modules are inherently configurable, aggregatable, portable, and extensible and singularly, or in combination (along with associated data), run as control methods under the VDE transaction operating environment." ('193 25:48-52) - ('193 77:12-27); ('193 83:11-22); ('193 181:20-21); ('193 272:29-36) - "Components 690 are preferably designed to be easily separable and individually loadable. ROS 602 assembles these elements together into an executable component assembly 690 prior to loading and executing the component assembly (e.g., in a secure operating environment such as SPE 503 and/or HPE 655)." ('193 83:43-48) - ('193 83:23); ('193 85:21-29 see '193 170:2-4); ('193 86:51-52); ('193 87:41-62); ('193 109:24-45); ('193 115:65-116:4); ('193 116:30-34); ('193 185:42-46) Extrinsic: Component: 1. Hardware or software that is part of a functional unit. 2. A functional part of an operating system. 3. A set of modules that performs a major function within a system. (IBM) Component: In data communications, a device or set of devices, consisting of hardware, along with its

Claim Term	MS Construction
	firmware, and or software that performs a specific function on a computer communications network. A Component is a part of a larger system, and may itself consist of other components. (Longley)
	"Thus, PERC 808 in effect contains a "list of assembly instructions" or a "plan" specifying what elements ROS 602 is to assemble together into a component assembly and how the elements are to be connected together. PERC 808 may itself contain data or other elements that are to become part of the component assembly 690." ('193 85:30-39)
contain, contained, containing 683.2, 912.8, 912.35	**Intrinsic:** - "Container 300y may contain and/or reference rules and control information 300y(1) that specify the manner in which searching and routing information use and any changes may be paid for." ('193 241:36-39) - "Each logical object structure 800 may also include a "private body" 806 containing or referencing a set of methods 1000 (i.e., programs or procedures) that control use and distribution of the object 300." ('193 128:25-28) - "Therefore, stationary object structure 850 does not contain a permissions record (PERC) 808; rather, this permissions record is supplied and/or delivered separately (e.g., at a different time, over a different path, and/or by a different party) to the appliance/installation 600. ('193 130:18-22) - "The content portion of a logical object may be organized as information contained in, not contained in, or partially contained in one or more objects." ('193 127:8-19) - "Therefore, stationary object structure 850 does not contain a permissions record (PERC) 808; rather, this permissions record is supplied and/or delivered separately (e.g., at a different time, over a different path, and/or by a different party)" ('193 130:18) - ('193 58:49-58); ('193 86:47-48); ('193 87:3-6); ('193 130:63-64); ('193 136:32-34); ('193 241:36-39); ('683 54:29-37) See also prior art referred to the relevant InterTrust patent file histories, e.g. U.S. Patent 5,715,403 **Extrinsic:** "Container: A contains protected *content*, which is divided into one or more *atomic elements*, and, optionally, *PERCs* governing the *content* and may be manipulated only as specified by a *PERC*." (ITG, 4/6/95, IT00028206, see footnote 2 and 4) "Container: A packaging mechanism, consisting of: *One or more Element-derived components. *An organization mechanism which provides a unique name within a flat namespace for each of the components in a Container." (ITG, 5/12/95, IT00028293) "Container: A protected digital information storage and transport mechanism for packaging content and control information." (ITG, 8/21/95, IT00032372, TD00068B) Container: A collection of content and control-related information. (IT VDE Container Overview, 2/10/95, IT00051228, ETM-9999 Version 0.21) Contain: In data security, a multilevel information structure. A container has a classification and may contain objects and/or other containers. (Longley, Information Security :Dictionary of Concepts, Standards, and Terms (1992) USP 5,369,702 Que's Computer Programmer's Dictionary ("Que") ("A dynamic data structure, the elements of which are arbitrary data items whose type is not known when the program is written." Dictionary of Computer Science Engineering and Technology (2001) ("Abstract data type storing a collection of objects (elements)") IT00037-44, IT002734-39, IT004188-96, IT0031572-85, IN00075960, IT00703055-71, IT0052146-64, IN00441189-224, IN0075983-87 See also Microsoft PLR 4-2 Exhs. E & F as revised, and InterTrust's Rule 30(b)(6) testimony.

Claim Term	MS Construction
control (n.) 193.1, 193.11, 193.15, 193.19, 891.1	Intrinsic: - "Claims ... are allowable over the prior art of record. The instant claims provide for first and second entity or control or procedure or executable code that are separately, remotely and different from each to combine or process or execute an operation or procedure based on at least first and second control or procedure or executable code in an electronic appliance or secure operating environment or third party different and remote from the first and second entity or control or procedure or executable code." 08/964,333 ('891), Office Action, 09/22/98, p. 3 (MSI028945) - "The virtual distribution environment 100 prevents use of protected information except as permitted by the "rules and controls" (control information)." ('193 56:26) - "As mentioned above, virtual distribution environment 100 "associates" content with corresponding "rules and controls," and prevents the content from being used or accessed unless a set of corresponding "rules and controls" is available." ('193 57:18-22) - "at least one rule and/or control associated with the software agent that governs the agent's operation." ('193 241:2-3) - "In this example control information may include one or more component assemblies that describe the articles within such a container (e.g. one or more event methods referencing map tables and/or algorithms that describe the extent of each article)." ('193 309:5-9) - ""Even if a consumer has a copy of a video program, she cannot watch or copy the program unless she has "rules and controls" that authorize use of the program. She can use the program only as permitted by the "rules and controls." ('193 53:60-63) - "A control set 914 contains a list of required methods that must be used to exercise a specific right (i.e., process events associated with a right)." ('193 151:14-16) - "If necessary, trusted go-between 4700 may obtain and register any methods, rules and/or controls it needs to use or manipulate the object 300 and/or its contents (FIG. 122 block 4778)." ('683, sheet 188) See also prior art referred to the relevant InterTrust patent file histories. MSI026598-602, 26626-7, 26630-42; MSI 028808-11, 28846-52, 28728-62, 28857-58, 28944-97, 28953-56 Extrinsic: Control: The determination of the time and order in which the parts of a data processing system and the devices that contain those parts perform the input, processing, storage, and output functions. (IBM) "5. Control Notes ... A Control must execute as a transaction ... A Control may require pre-conditions – that is that one or more other Controls have been executed before the Control is executed. [] 7. Control Execution Flow The following pseudocode describes the approximate execution sequence for a View Control [] 8. Operation of a Control (Execution of "Rules and Consequences") ..." (VDE Controls Notes, IT00051953-55) Control: A business rule that governs the use of content. (ITG, 1997-1998, ML00012B) Control: A set of rules and consequences that apply to a governed element. The term control can apply to either a control program or a control set. (ITG, 1997-2000, ML00012D) Control: *Control Element: A data structure that giverns (sic) the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). *Control mechanism: One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. * Control object: A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. *Control Parameter: A data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself. (ITG, 3/7/1995, IT00709618, see footnote 2) Control: Defines rules and consequences for operations on a Property Chunk. A Control may be

Claim Term	MS Construction
	implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node.(ITG, 5/12/95, IT00028293)

Control: A set of rules and consequences for operations on content, such as pricing, payment models, usage reporting etc. (ITG, 8/21/95, IT00032373, TD00068B)

Control: An object of the InterTrust Commerce Architecture that specifies business rules. Controls are applied at any time and at any point in the Chain of Handling and Control. InterTrust controls are dynamic, independent, and persistent. (ITG, 11/17/96, IT00035865, TD00189J)

"Rules and Controls" means any electronic information that directs, enables, specifies, describes, and/or provides contributing means for performing or not-performing, permitted and/or required operations related to Content, including, for example, restricting or otherwise governing the performance of operations, such as, for example, Management of such Content. (License Agreement, InterTrust/Universal Music Group, 4/13/99, Exhibit 11 to InterTrust 30(b)(6))

"A set of control elements corresponding to all of the property elements of a property. There may be zero or more controls for a given property." (IT 28204)

"Defines rules and consequences for operations on a Property Chunk . . . A single control applies to exactly one Property Chunk" (IT 28293)

"CONTROL(S): Controls refer to the rules and consequences associated with DigiBox containers. Controls may be applied dynamically. . ." (IT 35961)

"CONTROL: The rules associated with a governed entity such as a DigiBox container, property, or another control . . . applied dynamically. InterTrust controls are dynamic, independent, and persistent." (IT 35920)

". . . controls implement business rules" (IT 35892)

Webster's New World Dictionary of Computer Terms, 4th Ed. (1992) ("The function of performing required operations when certain specific conditions occur or when interpreting and acting upon instructions."); IT00125, IT31410-14, IT703083-89, IT51721-26, IT00735936 (key), IT51956 et seq., IN0075983-87, IN0075989-93; The Dictionary of Computing & Digital Media (1999) (control card)

See also Microsoft PLR 4-2 Exhs. E & F as revised, and InterTrust's Rule 30(b)(6) testimony. |
| controlling, control (v.)

861.58, 193.1 | Intrinsic:

-    "ROS 602 includes software intended for execution by SPU microprocessor 520 for, in part, controlling usage of VDE related objects 300 by electronic appliance 600. As will be explained, these SPU programs include "load modules" for performing basic control functions." ('193 66:5-8)
-    "VDE prevents many forms of unauthorized use of electronic information, by controlling and auditing (and other administration of use) electronically stored and/or disseminated information." ('193 11:60-63)
-    ('193 15:41-46); ('193 20:27-28); ('193 56:26-28); ('193 57:18-22) ('193 4:51-56); ('193 6:33-35); ('193 15:41-46); ('193 17:22-28); ('193 20:27-28)

Extrinsic:

Control: The determination of the time and order in which the parts of a data processing system and the devices that contain those parts perform the input, processing, storage, and output functions. (IBM)

Control: In data security, a multilevel information structure. A container has a classification and may contain objects and/or other containers. (Longley)

Control: A business rule that governs the use of content. (ITG, 1997-1998, ML00012B)

Control: A set of rules and consequences that apply to a governed element. The term control can apply |

Claim Term	MS Construction
	to either a control program or a control set. (ITG, 1997-2000, ML00012D)
	Control: *Control Element*: A data structure that governs (*sic*) the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). *Control mechanism*: One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. *Control object*: A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. *Control Parameter*: A data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself. (ITG, 3/7/1995, IT00709618, see footnote 2)
	Control: Defines rules and consequences for operations on a Property Chunk. A Control may be implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node. (ITG, 5/12/95, IT00028293)
	Control: A set of rules and consequences for operations on content, such as pricing, payment models, usage reporting etc. (ITG, 8/21/95, IT00032373, TD00068B)
copied file 193.11	Intrinsic: Extrinsic: Copy: A product of a document copying process.(IBM)
copy, copied, copying 193.1, 193.11, 193.15, 193.19	Intrinsic: - "These rights govern use of the VDE object 300 by that user or user group. For instance, the user may have an "access" right, and an "extraction" right, but not a "copy" right." ('193 159:23-26) - "At the same time, electronic testing will allow users to receive a copy (encrypted or unencrypted) of their test results when they leave the test sessions." ('193 319:12-15) - ('193 129:3-8); ('193 claim 60); ('193 53:60-62); ('193 131:65-132:1) Extrinsic: . Copy: A product of a document copying process.(IBM)
copy control 193.1	Intrinsic: - "If the user's budget permits the extraction ("yes" exit to decision block 2088), then the EXTRACT method 2080 creates a copy of the extracted object with specified rules and control information (block 2094). In the preferred embodiment, this step involves calling a method that actually controls the copy." ('193 194:36-42) Extrinsic: Copy Control: In the 3800 Printing Subsystem, the functions that determine the number of copies to be printed for each data set, and which copies will be printed with a forms overlay or have copy modification. (IBM) Control: A business rule that governs the use of content. (ITG, 1997-1998, ML00012B) Control: A set of rules and consequences that apply to a governed element. The term control can apply to either a control program or a control set. (ITG, 1997-2000, ML00012D) Control: *Control Element*: A data structure that governs (*sic*) the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). *Control mechanism*: One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. *Control object*: A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. *Control Parameter*: A

Claim Term	MS Construction
	data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself. (ITG, 3/7/95, IT00709618, see footnote 2)

Control: Defines rules and consequences for operations on a Property Chunk. A Control may be implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node.(ITG, 5/12/95, IT00028293)

Control: A set of rules and consequences for operations on content, such as pricing, payment models, usage reporting etc. (ITG, 8/21/95, IT00032373, TD00068B) |
| data item

891.1 | Extrinsic:
Data Item: 1. The smallest unit of named data that has meaning in the schema or subschema. 2. A unit of data, either a constant or a variable, to be processed. 3. In the AIX operating system, a unit of data to be processed that includes constants, variable, or array elements, and character substrings. 6. Synonymous with host variable. (IBM)

Data Item: In databases, the smallest unit of data that has independent meaning. (Longley)

Item List: A list of data included with various objects. Item lists take two forms. When they are first created, they are in the form of lists that contain one or more data items. When you are finished creating the list, you convert the list to a blob, which is a set of raw bits that store the data in a compact way. To retrieve items from the item list, you use the Interoperability Library item list functions, which convert the blob back to its interpreted list form and allow you to inspect the data items. (ITG, 1997-1998, ML00012B)

Data Item: An Element-derived bag of bits. (e.g., budget , meter, etc.) (ITG, 5/12/95, IT00028293) |
| derive, derives

900.155 | Intrinsic:

"Such control information can continue to manage usage of container content if the container is "embedded" into another VDE managed object, such as an object which contains plural embedded VDE containers, each of which contains content derived (extracted) from a different source." ('193 28:60-65)

Extrinsic: |
| descriptive data structure

861.58 | Intrinsic:

"The descriptive data structure can be used as a "template" to help create, and describe to other nodes, rights management data structures including being used to help understand and manipulate such rights management data structures." ('861 5:43-46)

"Claims [1,10,25,26] are rejected under 35 U.S.C. 102(b) as being clearly anticipated by the common and decades-old practice of using database schema to describe the structure of a database which requires password/identifications for access. ... Claims [1-17,25-26] are rejected under 35 U.S.C. 102(a) as being anticipated by Anderson et al (Anderson), USP 5,537,526, Method and Apparatus for Processing a Display Document Utilizing a System Level Document. The claims are rejected on the basis of the correspondence between the teachings of Anderson and the elements of the claims as follows: As to claim 1 (and 10), the TabstractModel 502 is a machine readable, abstract descriptive data structure which interoperates with Tmodels 506 (TM), and TmodelSurrogates 504 (TMS). ... These models are clearly data structures, and while they can be of many types, the data they manage can include restrictions that correspond to rights management." (08/805,804 ('861), Office Action, 06/25/98, p. 2-3)

- "The above-referenced Ginter et al. patent specification describes, by way of non-exhaustive |

Claim Term	MS Construction
	example, "templates" that can act as a set (or collection of sets) of control instructions and/or data for object control software. See, for example, the "Object Creation and Initial Control Structures," "Templates and Classes," and "object definition file," "information" method and "content" methods discussions in the Ginter et al. specification. The described templates are, in at least some examples, capable of creating (and/or modifying) objects in a process that interacts with user instructions and provided content to create an object. Ginter et al. discloses that templates may be represented, for example, as text files defining specific structures and/or component assemblies, and that such templates—with their structures and/or component assemblies—may serve as object authoring and/or object control applications. Ginter et al. says that templates can help to focus the flexible and configurable capabilities inherent within the context of specific industries and/or businesses and/or applications by providing a framework of operation and/or structure to allow existing industries and/or applications and/or businesses to manipulate familiar concepts related to content types, distribution approaches, pricing mechanisms, user interactions with content and/or related administrative activities, budgets, and the like. This is useful in the pursuit of optimized business models and value chains providing the right balance between efficiency, transparency, productivity, etc. The present invention extends this technology by providing, among other features, a machine readable descriptive data structure for use in association with a rights management related (or other) data structure such as a *secure container*." ('861 4:65) - "For example, the FIG. 2A example descriptive data structure headline definition 202a does not specify a particular headline (e.g., "Yankees Win the Pennant!"), but instead defines the location (for example, the logical or other offset address) within the container data structure 100a (as well as certain other characteristics) in which such headline information may reside." ('861 10:54-59); - "These descriptive data structure ("DDS") templates may be used to create containers." ('861 6:26-32); - "the descriptive data structure may be used in a creation process 302. The creation process 302 may read the descriptive data structure and, in response, create an output file 400 with a predefined format such as, for example, a container 100 corresponding to a format described by the descriptive data structure 200." ('861 11:60-64) - "The output of the layout tool 300 may be a descriptive data structure 200 in the form of, for example, a text file. A secure packaging process 302a may accept container specific data as an input, and it may also accept the descriptive data structure 200 as a read only input. The packager 302a could be based on a graphical user interface and/or it could be automated. The packager 302a packages the container specific data 314 into a secure container 100." ('861 12:9-16) - "FIG. 24 shows an example of a user data element (UDE") 1200 provided by the preferred embodiment. As shown in FIG. 24, UDE 1200 in the preferred embodiment includes a public header 802, a private header 804, and a data area 1206. The layout for each of these user data elements 1200 is generally defined by an SGML data definition contained within DTD 1108 associated with one or more load modules 1100 that operate on the UDE 1200." ('193 143:21-28) - "The publisher 3308 may create or otherwise provide content and/or VDE control structure templates that are delivered to the local repository 3302 for use by other participants who have access to the "internal" network. The templates may be used to describe the structure of containers, and may further describe whom in the publisher 3308's organization may take which actions with respect to the content created within the organization related to publication for delivery to (and/or referencing by) the repository 3302. For example, the publisher 3308 may decide (and control by use of said temple) that a periodical publication will have a certain format with respect to the structure of its content and the types of information that may be included (e.g. text, graphics, multimedia presentations, advertisements, etc.), the relative location and/or order of presentation of its content, the length of certain segments, etc. Furthermore, the publisher 3308 may, for example, determine (through distribution of appropriate permissions) that the publication editor is the only party that may grant permissions to write into the container, and that the organization librarian is the only party that may index and/or abstract the content." ('193 294:65-295:18) - "templates may be represented as text files defining specific structures and/or component

Claim Term	MS Construction
	assemblies. Templates, with their structure and/or component assemblies may serve as VDE object authoring or object control applications. ('193 260:36-47) - "...The result of object definition 1240 may be an object configuration file 1240 specifying certain parameters relating to the object to be created. Such parameters may include, for example, map tables, key management specifications, and event method parameters. The object construction stage 1230 may take the object configuration file 1240 and the information or content to be included within the new object as input, construct an object based on these inputs, and store object repository 728." ('193 103:38-46) - "In accordance with one example, the machine readable descriptive data structure provides a description that reflects and/or defines corresponding structure(s) within the rights management data structure. For example, the descriptive data structure may provide a recursive, hierarchical list that reflects and/or defines a corresponding recursive, hierarchical structure within the rights management data structure. In other examples, the description(s) provided by the descriptive data structure may correspond to complex, multidimensional data structures having 2,3, or n dimensions. The descriptive data structure may directly and/or indirectly specify where, in an associated rights management data structure, corresponding defined data types may be found. The descriptive data structure may further provide metadata that describes one or more attributes of the corresponding rights management data and/or the processes used to create and/or use it. In one example, the entire descriptive data structure might be viewed as comprising such metadata." ('861 5:57- 6:7) - ('193 245:44-51); ('683 32:41-53); ('861 5:25-41); ('861 10:49-59); ('861 12:9-11); ('861 13:21-27); ('861 20:25-47); ('193 259:37-51); ('193 298:41-62); ('193 103:3-32); ('193 285:9-35); ('193 193:49-59); ('193 287:37-41) Extrinsic:
designating 721.1	Intrinsic: Extrinsic:
device class 721.1	Intrinsic: "Furthermore, Applicants respectfully submit that some of the terms cited by the Examiner as "indefinite" are either well-known by persons skilled in the art or inherently clear. For example, in Claims 1-4, 22-25, the term "class" is used as part of the phrase "device class." Applicants respectfully submit that "device class" is inherently clear, meaning a group of devices which share at least one attribute." (08/689,754 ('721), Amendment, 04/14/99, p. 14) Extrinsic: Device: 1. A mechanical, electrical, or electronic contrivance with a specific purpose.(IBM) Device class: The generic name for a group of device types.(IBM) Device type: 1. The name for a kind of device sharing the same model number; for example, 2311, 2400, 2400-1. Contrast with device class. (2) The generic name for a group of devices; for example, 5219 for IBM 5219 Printers. Contrast with device class. (IBM)
digital file 193.1, 193.11, 193.15, 193.19	Intrinsic: Extrinsic: File: "A complete, named collection of information, such as a program, a set of data used by a program, or a user-created document. A file is the basic unit of storage that enables a computer to distinguish one set of information from another. A file is the "glue" that binds a conglomeration of instructions, numbers, words, or images into a coherent unit that a user can retrieve, change, delete, save, or send to an output device." (Microsoft Computer Dictionary, 3rd ed., 1997)
digital signature, digitally signing	Intrinsic: - "There exist many well known processes for creating digital signatures. One example is the Digital

Claim Term	MS Construction
721.1	Signature Algorithm (DSA). DSA uses a public-key signature scheme that performs a pair of transformations to generate and verify a digital value called a "signature." ('721 10:60-64) - ('721 4:64-67); ('721 11:7-22); ('721 14:49-60); ('721 14:64-15:2) - "Certificates play an important role in the trustedness of digital signatures, and also are important in the public-key authentication communications protocol (to be discussed below). In the preferred embodiment, these certificates may include information about the trustedness/level of security of a particular VDE electronic appliance 600 (e.g., whether or not it has a hardware-based SPE 503 or is instead a less trusted software emulation type HPE 655) that can be used to avoid transmitting certain highly secure information to less trusted/secure VDE installations." ('193 203:58-67) Extrinsic: Digital Signature: In computer security, encrypted data, appended to or part of a message, that enables a recipient to prove the identity of the sender. (IBM) Digital Signature: 1. In authentication, data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery. 2. In authentication, a data block appended to a message, or a complete encrypted message, such that the recipient can authenticate the message contents and/or prove that it could only have originated with the purported sender. (Longley) "Let B be the recipient of a message M signed by A, then A's [digital] signature must satisfy three requirements: 1. B must be able to validate A's signature on M. 2. It must be impossible for anyone, including B, to forge A's signature. 3. In case A should disavow signing a message M, it must be possible for a judge or third party to resolve a dispute arising between A and B. A digital signature therefore establishes sender authenticity [] it also establishes data authenticity." (Denning, p. 14)[7] "A cipher in unconditionally secure if, no matter how much ciphertext is intercepted, there is not enough information in the ciphertext to determine the plaintext uniquely." (Denning, p.5) (Davies, p. 41, 380) "A cipher is computationally secure, or strong, if it cannot be broken by systematic analysis with available resources." (Denning, p.5) (Davies, p.41, 370)
entity's control 891.1	Intrinsic: - "A public-key certificate is someone's public key "signed" by a trustworthy entity such as an authentic PPE 650 or a VDE administrator. " ('193 203:42-45) - "Distribution involves three types of entity. Creators usually are the source of distribution. The typically set the control structure "context" and can control the rights which are passed into a distribution network. Distributors are users who form a link between object (content) end users and object (content) creators. They can provide a two-way conduit for rights and audit data. Clearinghouses may provide independent financial services, such as credit and/or billing services, and can serve as distributors and/or creators. Through a permissions and budgeting process, these parties collectively can establish fine control over type and extent of rights usage and/or auditing activities." ('193 267:34-45) Extrinsic: Control: A business rule that governs the use of content. (ITG, 1997-1998, ML00012B) Control: A set of rules and consequences that apply to a governed element. The term control can apply

---

[7] "Denning" herein refers to Denning, D., Cryptography and Data Security, 1983, MSI085569.

Claim Term	MS Construction
	to either a control program or a control set. (ITG, 1997-2000, ML00012D)
	Control: *Control Element:* A data structure that giverns (*sic*) the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). *Control mechanism:* One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. * *Control object:* A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. *Control Parameter:* A data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself. (ITG, 3/7/95, IT00709618, see footnote 2)
	Control: Defines rules and consequences for operations on a Property Chunk. A Control may be implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node. (ITG, 5/12/95, IT00028293)
	Control: A set of rules and consequences for operations on content, such as pricing, payment models, usage reporting etc. (ITG, 8/21/95, IT00032373, TD00068B)
environment 912.35, 900.155, 891.1, 683.2, 721.34	Intrinsic: '721 file history Rejection 10/15/98, Amendment 4/19/99 at 13-15
	Extrinsic:
	"Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment.*" (ITG, 8/21/95, IT00032375, TD00068B)
executable programming, executable 912.8, 912.35, 721.34	Intrinsic:
	- "Furthermore, applicants' independent claims 16, 36, 37 and 64 require secure delivery and use of plural executable items. See claim 16 ("securely delivering a first procedure ... securely delivering ... a second procedure separable or separate from said first procedure..."); claim 36 ("securely delivering plural executable procedures ..."), claim 37 ("securely delivering a first piece of executable code ... securely delivering a second piece of executable code ...") and claim 64 ("securely receiving a first load module ... securely receiving a second load module ..."). These features are not taught or suggested by either Rosen or Johnson. Johnson's databases comprise data, not executable code."
	(08/388,107, Amendment, 06/20/97, p. 24-25) (MSI028848-49)
	"In addition, Applicants would like to draw the Examiner's attention to other sections of the specification in support of words or phrases cited by the Examiner as "indefinite." ... The noun "executable," as used in Claims ... 34-36 ..., is defined in the specification on page 7." (pg. 13-14) (page 7 of the original specification is '721 2:62-3:13 of the issued patent) (08/689,754 ('721), Amendment, 04/14/99, p. 14)
	Extrinsic:
	Execute: 1. To perform the actions specified by a program or a portion of a program.(IBM)
	Executable: 1. Program that has been link-edited and therefore can be run in a processor; The set of machine language instructions that constitute the output from the compilation of a source program.(IBM)
	Executable Programming: 1. A program that has been link-edited and therefore can be run in a processor. 2. The set of machine language instructions that constitute the output from the compilation of a source program.(IBM)
execution space, execution space	Intrinsic:
	- "One important security layer involves ensuring that certain component assemblies 690 are formed,

Claim Term	MS Construction
identifier 912.8	loaded and executed only in secure execution space such as provided within an SPU 500." ('193 87:35-38) - "The following is an example of a possible field layout for load module public header 802: ... Execution Space Code: Value that describes what execution space (e.g., SPE or HPE) this load module (sic)." ('193 140:15-35) - "The Ginter et al. patent disclosure describes, among other things, techniques for providing a secure, tamper resistant execution spaces within a "protected processing environment" for computer programs and data. The protected processing environment described in Ginter et al. may be hardware-based, software-based, or a hybrid. It can execute computer code the Ginter et al. disclosure refers to as "load modules."" ('721 3:16-23) "Furthermore, Applicants respectfully submit that some of the terms cited by the Examiner as "indefinite" are either well-known by persons skilled in the art or inherently clear. ... Furthermore, Applicants respectfully submit that the term "execution spaces," as used in Claim 32, is well-known in the art. It refers to a resource which can be used for execution of a program or process." 08/689,754 ('721), Amendment, 04/14/99, p. 14 - ('193 86:39-47); ('193 88:38-43); ('193 104:39-44); ('193 140:37-50) - "The SPE (HPE) load module execution manager ("LMEM") 568 loads executables into the memory managed by memory manager 578 and executes them. LMEM 568 provides mechanisms for tracking load modules that are currently loaded inside the protected execution environment. LMEM 568 also provides access to basic load modules and code fragments stored within, and thus always available to, SPE 503. LMEM 568 may be called, for example, by load modules 1100 that want to execute other load modules." ('193 111:20-28) - "The internal ROM 532 and RAM 534 within SPU 500 provide a secure operating environment and execution space." ('193 69:33-35) - SPU 500 general purpose RAM 534 provides, among other things, secure execution space for secure processes. ('193 70:43-44) Extrinsic: Execution: The process of carrying out an instruction or instructions of a computer program by a computer.(IBM) Tanenbaum
governed item 683.2	Intrinsic: - See "Allow" - "If an image representation of a signature is stored on portable media or in a directory service, the image may be stored in an electronic container 302. Such a container 302 permits the owner of the signature to specify control information that governs how the signature image may be used." ('683 27:29-) - VDE control information which governs the use, and consequences of use, of VDE controlled content." ('193 288:5-12) - ('193 128:41-45) Extrinsic: Govern: To initiate the execution of controls. (ITG, 10/2/96, IT00035894, TD00189F) Governance: The act of applying controls. Governance is the fundamental activity of the InterTrust Commerce Architecture. (ITG, 11/17/96, IT00035867, TD00189J) Governed Element: An InterTrust Commerce Architecture object to which governance is applied. DigiBox containers, content, control sets, and control records are the primary examples of governed

Claim Term	MS Construction
	elements. (ITG, 11/17/96, IT00035867, TD00189J)
	Defined consistent (IT 35962)
Halting 900.155	Intrinsic: - "Dynamic Check of Association Between Appliance and PPE Instance: The executing operational materials 3472 may next compare an embedded electronic appliance signature SIG' against the electronic appliance signature SIG stored in the electronic appliance itself (FIG. 69K, decision block 3564). As discussed above, this technique may be used to help prevent operational materials 3472 from operating on any electronic appliance 600 other than the one it was initially installed on. PPE 650 may disable operation if this machine signature check fails ("no" exit to decision block 3564, FIG. 69K; disable block 3566)." ('900 243:30-41) "When an inconsistency is detected ("yes" exit to decision block 3590, FIG. 69L), PPE 650 can take appropriate action such as locking itself up from further use until reconstructed under the trusted server's control (FIG. 69L, disable block 3591)." ('900 247:50-54) Extrinsic: Halt Indicators: In RPG, an indicator that stops the program when an unacceptable condition occurs. Valid halt indicators are H1-H9 (IBM) Halt Instruction: 1. A machine instruction that stops execution of a program. 2. Synonym for pause instruction. .(IBM)
host processing environment 900.155	Intrinsic: - ('193 63:13-17); ('193 79:60-67); ('193 81:4-8); ('900 230:57-61); ('900 231:23-31); ('900 236:505-53) - "HPE(s) 655 and SPE(s) 503 are self-contained computing and processing environments that may include their own operating system kernel 688 including code and data processing resources." ('193 79:36-39) - "HPEs 655 may be provided in two types: secure and not secure." ('193 80:8-9) - ('193 79:31); ('193 80:22-36); ('193 80:40-65, Fig. 10); ('193 88:31-43); ('193 104:39-44) Extrinsic: Host processor : 1. A processor that controls all or part of a user application network. 2. In a network, the processing unit in which resides the access method for the network. 4. A processing unit that executes the access method for attached communication controllers.(IBM) "Host Processing Environment (HPE): A software-only realization of the PPE, protected from tampering by appropriate software techniques. No longer preferred because of the potential confusion between the "H" in the acronym and "H" as in "Hardware" (which this isn't). [REPLACEMENT UNCERTAIN]" (ITG, 3/7/95, IT00709621)[8] "Secure Processing Environment (SPE): A hardware-supported realization of the PPE, protected from tampering by physical security techniques. No longer preferred because of the potential confusion between the "S" in the acronym and "S" as in "Software" (which this isn't). [REPLACEMENT UNCERTAIN]" (ITG, 5/12/95, IT00028302) Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment*. (ITG, 8/21/95, IT00032375, TD00068B)
identifier, identify,	Intrinsic:

Claim Term	MS Construction
identifying 193.11, 193.15, 912.8, 912.35, 861.58	- "Portable appliance 2600 RAM 534 may contain, for example, information which can be used to uniquely identify each instance of the portable appliance. This information may be employed (e.g. as at least a portion of key or password information) in authentication, verification, decryption, and/or encryption processes." ('193 230:22-27) - ('193 25:31-38); ('193 37:27-31); ('193 111:47-67) ('193 111:59-67); ('193 124:8-18); ('193 131:40-45); ('193 139:41-55); ('193 214:39-41) ('861 12:63-13:4); ('193 67:21-26); ('193 209:63-67); ('193 214:39-41) Extrinsic: Identifier: 1. One or more characters used to identify or name a data element and possibly to indicate certain properties of that data element. 2. In programming languages, a token that names a data object such as a variable, an array, a record, a subprogram or a function. (IBM) Identifier: 1. In computing, a character or group of characters used to identify, indicate or name a body of data. 2. In computing, a name or string of characters employed to identify a variable, procedure, data structure or some other element of a program. (Longley)
including 193.1 (at 320:63, and 321:3); 193.19 (at 324:15); 912.8 (at 327:36, 39, and 41); 912.35 (330:35 and 39); 861.58 (at 26:53 and 63); and 683.2 (at 63:60).	Intrinsic: - Prosecution History of '900 Patent: Changed "including" to "comprising" "to avoid any possible ambiguity relating to whether the control information must be 'inside' the secure object." Amendment to allowed claim 60, 10/29/98. - "Load modules 1100 in the preferred embodiment comprise executable code, and may also include or reference one or more data structures called "data descriptor" ("DTD") information." ('193 136:53-56) - "include or reference" ('861 15:21) - "including or addressing" (claim 58); - "includes a reference to" (claim 69); - "Secure database 610 in the preferred embodiment does not include VDE objects 300, but rather references VDE objects stored, for example, on file system 687 and/or in a separate object repository 728." ('193 126:26-65) - ('193 131:18-20) Extrinsic: "3. To consider with or place into a group, class, or total: thanked the host for including us." (Amer. Heritage Dictionary, 4th ed.)
information previously stored 900.155	Intrinsic: Extrinsic: Information: 1. In information processing, knowledge concerning such things as facts, concepts, objects, events, ideas, and processes, that within a certain context has a particular meaning. (IBM) Information: 1. Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape. 3. Knowledge that was unknown to the receiver prior to its receipt. Information can only be derived from data that is accurate, timely, relevant and unexpected.(Longley) Store: 1. To place data into a storage device. 2. To retain data in a storage device.

Claim Term	MS Construction
integrity programming 900.155	**Intrinsic:** - "Upon initialization, the operational materials 3472 validate the embedded signature value against the actual electronic appliance 600 signature SIG, and may refuse to start if the comparison fails." ('900 239:21-25)[i] - "an otherwise unused section of the non- volatile CMOS RAM 656a may be used to store a signature 3497d. Signature 3497d is verified against the PPE 650's internal state whenever the PPE is initialized." ('900 239:51-55) - "Dynamic Check of Association Between Appliance and PPE Instance: The executing operational materials 3472 may next compare an embedded electronic appliance signature SIG' against the electronic appliance signature SIG stored in the electronic appliance itself (FIG. 69K, decision block 3564). As discussed above, this technique may be used to help prevent operational materials 3472 from operating on any electronic appliance 600 other than the one it was initially installed on. PPE 650 may disable operation if this machine signature check fails ("no" exit to decision block 3564, FIG. 69K; disable block 3566)." ('900 243:30-41) - ('193 80:45-48) **Extrinsic:** Integrity: The protection of systems, programs, and data from inadvertent or malicious destruction or alteration.(IBM) Integrity: 1. In data security, that computer security characteristic that ensures that computer resources operate correctly and that the data in the databases are correct. 2a. In data security, the capability of an automated system to perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. 2b. In data security, inherent quality of protection that ensures and maintains the security of entities of a computer system under all conditions.(Longley) Programming: 1. A sequence of instructions suitable for processing by a computer. 2. In programming languages, a logical assembly of one or more interrelated modules. 4. A sequence of instructions that a computer can interpret and execute.(IBM) Programming: The process by which a computer is made to perform a specialized task. It involves the creation of a formalized sequence of instructions which can be recognized and implemented by the machine. (Longley) Integrity: The ability to verify that data is unmodified from its intended value. (ITG, 5/12/95, IT00028294) Integrity: In relation to digital content, a state in which that content is unmodified and operations on the content are performed only as specified by the rightsholders. DigiBox containers ensure integrity. (ITG, 10/2/96, IT00035895, TD00189F) Integrity: definition varies slightly, best seems to be – A state in which content is unmodified and operations on properties are performed only as specified by the rights holders (IT 35922). Integrity: The assurance that content in a DigiBox container or content being processed by an IT content node has not been tampered with. (IT 35868)
key 193.19	**Intrinsic:** "Key Types The detailed descriptions of key types below further explain secret-key embodiments; this summary is not intended as a complete description. The preferred embodiment PPE 650 can use different types of keys and/or different "shared secrets" for different purposes. Some key types apply to a Public-Key/Secret Key implementation, other keys apply to a Secret Key only implementation, and still other key types apply to both. The following table lists examples of various key and "shared secret"

Claim Term	MS Construction
	information used in the preferred embodiment, and where this information is used and stored:

```
                                    Used in PK or    Example Storage
        Key/Secret Information Type  Non-PK             Location(s)
        Master Key(s) (may include   Both              PPE
        some of the specific keys                      Manufacturing facility
        mentioned below)        .                      VDE administrator
        Manufacturing Key            Both (PK          PPE (PK case)
                                     optional)         Manufacturing facility
        Certification key pair       PK         .      PPE
                                                       Certification repository
        Public/private key pair      PK                PPE
                                                       Certification repository
                                                       (Public Key only)
        Initial secret key           Non-PK            PPE
        PPE manufacturing ID         Non-PK            PPE
        Site ID, shared code, shared Both         . .    PPE
        keys and shared secrets
        Download authorization key   Both              PPE
                                                       VDE administrator
        External communication       Both              PPE
        keys and other info                            Secure Database
        Administrative object keys   Both               Permission record
        Stationary object keys       Both              Permission record
        Traveling object shared keys Both                 Permission record
        Secure database keys    .    Both         .    PPE
        Private body keys            Both              Secure database
                                                    .  Some objects
        Content keys            .    Both              Secure database
                                                       Some objects
        Authorization shared secrets Both                 Permission record
        Secure Database Back up      Both              PPE
        keys  .                                        Secure database"
```
('193 211:32 – 212:11)

- ('193 211:18-212:18); ('193 193:8-23); ('193 207:50-60); ('193 208:38-40)

Extrinsic:

Keys: The permissions record also contains the fundamental decryption keys for an object. It may contain the keys for the object content or keys to decrypt portions of the object that contain other keys that then can be used to decrypt the content of the object. Usage of the keys is controlled by the Control Sets in the same permissions record. There are many more aspects to the keys in the permissions record that are beyond the scope of this document. (VDE ROI DEVICE v1.0a 9 Feb 1994, IT00008601)

Key: 7. In computer security, a sequence of symbols used with a cryptographic algorithm for encrypting or decrypting data. (IBM)

Key: 1. In cryptography, a sequence of symbols that controls the operations of encipherment and decipherment. 2. In cryptography, a symbol or sequence of symbols (or electrical or mechanical correlates of symbols) that control the operations of encryption and decryption). (Longley)

load module 912.8, 721.1	Intrinsic: Prosecution History of Application 08/388,107 ('912 Patent is continuation) "Furthermore, applicants' independent claims 16, 36, 37 and 64 require secure delivery and use of plural executable items. See claim 16 ("securely delivering a first procedure ... securely delivering ... a second procedure separable or separate from said first procedure..."); claim 36 ("securely delivering plural executable procedures ..."), claim 37 ("securely delivering a first piece of executable code ... securely delivering a second piece of executable code ...") and claim 64 ("securely receiving a first

Claim Term	MS Construction
	load module ... securely receiving a second load module ..."). These features are not taught or suggested by either Rosen or Johnson. Johnson's databases comprise data, not executable code."

08/388,107, Amendment, 06/20/97, p. 24-25 (MSI028848-49)

- "Load module 1100 contains code and static data (that is functionally the equivalent of code), and is used to perform the basic operations of VDE 100. Load modules 1100 will generally be shared by all the control structures for all objects in the system, though proprietary load modules are also permitted. Load modules 1100 may be passed between VDE participants in administrative object structures 870, and are usually stored in secure database 610. They are always encrypted and authenticated in both of these cases. When a method core 1000' references a load module 1100, a load module is loaded into the SPE 503, decrypted, and then either passed to the electronic appliance microprocessor for executing in an HPE 655 (if that is where it executes), or kept in the SPE (if that is where it executes)." ('193 139:19-32)

- ('193 20:27-30); ('193 71:19-40); ('193 77:12-29) ('193 86:49-60); ('193 87:41-62); ('193 109:24-45); ('193 111:20-28); ('193 111:29-39); ('193 111:40-47); ('193 111:59-67); ('193 126:30); (193 139:28-31); ('193 139:60-140:6); ('193 140:1-6); ('193 140:44-50); ('193 141:42-55); ('193 209:52-210:35); ('193 17:15-17); ('193 20:27-30); ('193 86:39-48); ('193 139:41-51); ('193 151:20-22); ('721 3:21-35)

Extrinsic:

Load module: 1. All or part of a computer program or subprogram in a form suitable for loading into main storage for execution by a computer; usually the output of a linkage editor.(IBM)

Load Module: A procedure, dynamically loaded or resident within the PPE, that performs or controls operations within the PPE. Some load modules are associated with individual objects or types of objects; others perform general utility operations. (ITG, 3/7/95, IT00709618 see footnote 2)

"Load Module: shall mean an executable program that, when combined with control data and/or parameters, forms procedures or programs for performing specific types of control functions in compliance with EPR Specifications. Load Modules and their executable programs and associated control data and/or parameters are designed to, at least in part, be employed as one or more control elements which are used within a protected information transaction/distribution management arrangement." (License Agreement between National Semiconductor and EPR, 3/18/94, Exhibit 12 to InterTrust 30(b)(6))

"Load Module: The lowest level of a VDE control structure: an executable program that operates, under control of a *method* or another *load module,* to manipulate VDE-protected elements (which may be in *containers* otherwise)." (IT VDE Container Overview, 2/10/95, IT00051228, ETM-9999 Version 0.21)

"A load module is an executable program that manipulates VDE elements and content to perform a specific control function. A load module invoked as an external method is responsible for ensuring that all its related load modules, methods, elements, etc. are available and that all required option choices have been made." (IT VDE Container Overview, 2/10/95, IT00051234, ETM-9999 Version 0.21) |
| Machine check programming

900.155 | Intrinsic:

- "machine check" does not appear in specification
- "Correspondence Between Installed Software and Appliance "Signature". Another technique that may be used during the installation routine 3470 is to customize the operational materials 3472 by embedding a "machine signature" into the operational materials to establish a correspondence between the installed software on a particular electronic appliance 600 (FIG. 69C, block 3470(7)). ('900 239:4-14)
- For electronic appliances 600 where it is feasible to do so, the installation procedure 3470 may determine unique information about the electronic appliance 600 (e.g., a "signature" SIG in the sense of a unique value—not necessarily a "digital signature" in the cryptographic sense)." ('900 239:15-19) |

Claim Term	MS Construction
	- "FIG. 69G shows an example of some of these appliance-specific signatures." ('900 239:41-42) - "Dynamic Check of Association Between Appliance and PPE Instance: The executing operational materials 3472 may next compare an embedded electronic appliance signature SIG' against the · electronic appliance signature SIG stored in the electronic appliance itself (FIG. 69K, decision block 3564). As discussed above, this technique may be used to help prevent operational materials 3472 from operating on any electronic appliance 600 other than the one it was initially installed on. PPE 650 may disable operation if this machine signature check fails ("no" exit to decision block 3564, FIG. 69K; . disable block 3566)." ('193 243:30-) - "Signature 3497d may also be updated whenever a significant change is made to the secure database 610. If the CMOS RAM signature 3497d does not match the database value, PPE 650 may take this mismatch as an indication that a previous instance of the secure database 610 and/or PPE 650 software has been restored, and appropriate action can be taken. ('900 239:55-240:6) - ('900 240:15-26); (900 Claim 183) Extrinsic: Machine check: An error condition that is caused by an equipment malfunction. (IBM)
Metadata information 861.58	Intrinsic: - "This metadata can define certain characteristics associated with the object name. For example, such metadata may impose integrity or other constraints during the creation and/or usage process (e.g., "when you create an object, you must provide this information", or "when you display the object, you must display this information"). The metadata 264 may also further describe or otherwise qualify the associated object name." ('861 15:21-31) - (861 Abstract); ('861 6:2-7); ('861 8:57-64); ('861 13:30-34); ('861 14:7-11); ('861 16:37-52) Extrinsic: Metadata: In databases, data that describe data objects. (IBM) Information: 1. In information processing, knowledge concerning such things as facts, concepts, objects, events, ideas, and processes, that within a certain context has a particular meaning.(IBM) Metadata: 1. In computing, data referring to other data (such as data structures, indices, and pointers) that are used to instantiate an abstraction (such as 'process,' 'task,' 'segment,' 'file,' or 'pipe') 2. In computing, a special database, also referred to as a data dictionary, containing descriptions of the elements. (Longley)
opening secure containers 683.2	Intrinsic: - "Because container 152 can only be opened within a secure protected processing environment 154 that is part of the virtual distribution environment described in the above-referenced Ginter et al. patent disclosure" ('712 168:22-25) - Special mathematical techniques known as "cryptography" can be used to make electronic container 302 secure so that only intended recipient 4056 can open the container and access the electronic document (or other item) 4054 it contains. ('683 15:67-16:4) - The appliance 600 may then open the secure electronic container ("attaché case") 302 and deliver the item it contains to recipient 4056 (FIG. 91B, block 4092D). ('683) - Appliance 600 may then generate a "send" or "open" event to PPE 650 requesting the PPE to open container 302 and allow the user to access its contents. - ('193 185:7-30); ('193 185:42-46); ('683 19:27-32); ('193 183:28-29); ('193 183:55-57); ('193 185:11-16) Extrinsic: Open: 1. The function that connects a file to a program for processing. 4. To prepare a file for

Claim Term	MS Construction
	processing. (IBM)
	Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM)
	Container: In data security, a multilevel information structure. A container has a classification and may contain objects and/or other containers. (Longley)
	Container: contains protected content which is divided into one or more atomic elements, and optionally, PERCs governing the content and may be manipulated only as specified by a PERC. (ITG, 3/7/1995, IT00709616)
	Container: A protected (encrypted) storage object that incorporates descriptive information, protected content, and (optionally) control objects applicable to that content. (ITG, 3/7/1995, IT00709617, see footnote 3)
	Container: A protected digital information storage and transport mechanism for packaging content and control information. (ITG, 8/21/95, IT00032372, TD00068B]
operating environment 891.1	Intrinsic: Extrinsic: Operating Environment: The physical environment; for example, temperature, humidity, and layout.(IBM) Operating system: In computing, a collection of software programs intended to directly control the hardware of a computer and on which all the other programs running on the computer generally depend.(Longley) Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment*. (ITG, 8/21/95, IT00032375, TD00068B) Operation: A manipulation of some protected resource (e.g., content in a *container* or control records in a *PERC*) (IT VDE Container Overview, 2/10/95, IT00051228, ETM-9999 Version 0.21)
organization, organization information, organize 861.58	Intrinsic: - "a descriptive data structure could serve as 'instructions' that drive an automated packaging application for digital content and/or an automated reader of digital content such as display priorities and organization (e.g., order and/or layout)."('861 7:54-57); - For example, the descriptive data structure may provide a recursive, hierarchical list that reflects and/or defines a corresponding recursive, hierarchical structure within the rights management data structure ('861 5:57-63) ". ... descriptive data structure may directly and/or indirectly specify where, in an associated rights management data structure, corresponding defined data types may be found." ('861 5:67-6:2); - Issued claim 1: a first memory storing a descriptive data structure, said descriptive data structure including: information regarding a first organization of elements within a secure container, said information including: information on the organization of said elements within said secure container; and information on the location of at least some of said elements within said secure container" - Issued claim 34: "a representation of the format of data contained in a first rights management data structure said representation including: element information contained within said first rights management data structure; and organization information regarding the organization of said elements within said first rights management data structure; and information relating to metadata, said metadata including" - Issued claim 45 (dependent from 34-44): "said information regarding elements contained within said first rights management data structure includes information relating to the location of at least one such element." - Issued claim 73: "said descriptive data structure organization information includes information

Claim Term	MS Construction
	specifying that said first secure container contents will include at least a title and a text section referred to by said title." - Issued claim 74: "said descriptive data structure organization information includes information specifying that said first secure container contents will include at least one advertisement." - Issued claim 75: "said descriptive data structure further includes information relating to the location at which said title, said text section and said advertisement should be stored in said first secure container." - Issued claim 76: "at least a portion of said descriptive data structure organization information includes information specifying fields relating to at least one atomic transaction" ('193 103:23-46) Extrinsic:
portion 193.1, 193.11, 193.15, 193.19, 912.8, 912.35, 861.58	Intrinsic: Extrinsic: Portion: "1. A section or quantity within a larger thing; a part of a whole. 2. A part separated from a whole." (American Heritage Dictionary 4th Ed.)
prevents 721.34	Intrinsic: - "VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users." ('193 4:51-56) - "VDE ensures that certain prerequisites necessary for a given transaction to occur are met." ('193 20:27-28) - "For example, shrink-wrapping does not prevent the constant illegal pirating of software once removed from either its physical or electronic package." ('193 5:60-62) "VDE, for example, provides the ability to prevent, or impede, interference with and/or observation of, important rights related transactions and processes. VDE, in its preferred embodiment" ('193 4:1-4) "After receiving enabling distribution control information from creator A, distributor A may manipulate an application program to specify some or all of the particulars of usage control information for users and/or user/distributors enabled by distributor A (as allowed, or not prevented, by senior control information)." ('193 303:63) - ('193 6:33-35); ('193 15:41-46); ('193 17:22-28); ('193 309:10-16); ('193 303:63-304:1) Extrinsic:
processing environment 912:35, 900:155, 721:34, 683.2	Intrinsic: - "Another approach to supporting COTS software would use the VDE software running on the user's electronic appliance to create one or more "virtual machine" environments in which COTS operating system and application programs may run, but from which no information may be permanently stored or otherwise transmitted except under control of VDE." ('193 279:26-40) - "VDE may be combined with, or integrated into, many separate computers and/or other electronic appliances. These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc. The secure subsystem in the preferred embodiment comprises one or more "protected processing environments", ..." ('193 9:22) - ('193 9:22-29); ('683 24:26-33); ('193 60:51-64)

Claim Term	MS Construction
	Extrinsic: Processing: 1. The performance of logical operations and calculations on datum including temporary retention of data in processor storage while the data is being operated on.(IBM) Process: (1) in computing, the active system entity through which programs run. The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system. 2. In computing, a program in execution. ... (4) In computing, a program is a static piece of code and a process is the execution of that code. (Longley) Environment: 1. The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system. 2. In computer security, those factors, both internal and external, of an ADP system that help to define the risks associated with its operation (Longley) Secure Processing Environment (SPE): A hardware-supported realization of the PPE, protected from tampering by physical security techniques. No longer preferred because of the potential confusion between the "S" in the acronym and "S" as in "Software" (which this isn't). [REPLACEMENT UNCERTAIN] (ITG, 5/12/95, IT00028302) Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment.* (ITG, 8/21/95, IT00032375, TD00068B)

protected processing environment 721:34, 683.2	See also "secure"
	
	Intrinsic:
	
	Prosecution History of Application 08/778,256 (continuation of '891 Patent, issued at USP 5,949,876)
	
	    "Independent claims 65 and 76 each recite a "protected processing environment." ... Griffeth et al. [U.S. Pat. No. 5,505,837], Yamamoto [U.S. Pat. No. 5,508,913] and Wyman [U.S. Pat. No. 5,260,999] do not disclose these aspects of these claims.
	    The system disclosed in Griffeth et al is designed to allow negotiation to proceed in an environment in which a negotiating party does not disclose information about its negotiation goals to the other negotiating party. ... Griffeth et al. does not disclose any privacy protection mechanism and neither teaches nor suggests any secure processing environment or that any operations (e.g., integration or execution) occur securely. Indeed, Griffeth contains no suggestion that any protection mechanism is needed to maintain negotiation goals in privacy, since Griffeth does not suggest that the other party may try to improperly discover information which is intended to remain private.
	    Yamamoto states the following: "Here, the data is enciphered by the data encipher apparatuses 26 so as to maintain confidentiality." Col. 3, lines 46-47. Since Yamamoto makes no other reference to the encipherment, or to the apparatuses 26, it is impossible to determine how the data encipherment is used, or the roles it plays in the disclosed apparatus. From an examination of Fig. 3, however, it appears that the data encipher apparatuses 26 are placed on connections between a particular site and other, physically separated sites. For example, customer office 23b is connected to sub-center 22 by a line, which apparently represents a communication path. That line connects directly to a data encipher apparatus 26 in customer office 23b, and to another data encipher apparatus 26 in sub-center 22.
	    Thus, it appears that the data encipher apparatuses 26 are used, in some undisclosed manner, to encipher at least some data which travels among physically separated locations. It is possible to imagine, for example, that data is enciphered prior to being sent out on an insecure public transmission line, and is then deciphered once received in a new location.
	    Yamamoto does not disclose, however, that the processing environments are themselves secure, or that either execution or integration occur in a secure manner or in a secure environment. Indeed, Yamamoto contains no suggestion that security within a processing environment would even be desirable. By suggesting that data is deciphered once it enters an office (e.g., office 23b), in fact, Yamamoto teaches away from a secure environment, since it would appear that the data is used "in the clear" within the office, with no suggested protection beyond a simple password for the computer.

Claim Term	MS Construction

Wyman is equally deficient regarding these elements. Although Wyman specifies that a license may contain a digital signature, therefore rendering the license unforgeable (Col. 14, lines 24-54), Wyman neither teaches nor suggests that the processing environment is itself secure or that any operations occur in a secure manner. The Wyman digital signatures no more suggest a secure processing environment than the requirement that paper contracts be signed in ink suggests that the contracts will be created, read or negotiated in a secure location."

08/778,256 ('876), Amendment, 01/20/98, p. 58-60

- "The role of go-between 4700 may, in some circumstances, be played by one of the participant's SPU's 500 (PPEs), since SPU (PPE) behavior is not under the user's control, but rather can be under the control of rules and controls provided by one or more other parties other than the user (although in many instances the user can contribute his or her own controls to operate in combination with controls contributed by other parties)." ('683 24:26)

- "SPU 500 provides a tamper-resistant protected processing environment ("PPE") in which processes and transactions can take place securely and in a trusted fashion." ('683 16:60-62)
- "The computer 3372 may then execute the operational materials 3472 from its hard disk 3376 to provide software-based protected processing environment 650 and associated software-based tamper resistant barrier 672) ('900 231:27-31));
- ('193 20:58-63); ('193 21:11-17); ('721 7:19-23); ('721 16:64-17:5);

- "HPE(s) 655 and SPE(s) 503 are self-contained computing and processing environments that may include their own operating system kernel 688 including code and data processing resources." ('193 79:36-39)

- (see Figs. 10 and 13), ('193 79:24), (105:23, 105:43, 109:46); ('193 13:7-23); ('193 223:30-44)

- "In one example, a person with a laptop 5102 or other computer lacking a PPE 650 wishes nonetheless to take advantage of a subset of secure item delivery services." ('683 62:17-20)

"Claims 7-11, ... 99-111 ... are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (5,412,717) in view of Narasimhalu et al (5,499,298). Fischer discloses a method and apparatus including a system monitor which limits the ability of a program about to be executed to the use of predefined resources, ... The set of authorities and restrictions are referred to as "program authorization information" or "PAI". ... A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. ... memory containing a first rule corresponds to a first PAI under a first PCB ... ... Here, Fischer provides a secure container in the form of a program, i.e. a governed item, having an associated PAI, i.e. at least one rule associated with the secure container. A protected processing environment ("PPE") protecting at least some information contained in the PPE, see Fischer Terminal A, and including hardware and/or software used for applying said first rule and the secure container in combination to at least in part govern at least one aspect of access to or use of the governed item, see Fischer at Figure 5 and column 10, lines 8-39 where the first rule in memory is first PCB providing a first PAI and the secure container is a program associated with a second PCB providing a first PAI and the secure container is a program associated with a second PCB having a second PAI associated with the governed item, i.e. the program. ... The difference between claim 7 and Fischer is that the PPE disclosed in Fischer is not explicitly disclosed as protected from tampering by a user of the first apparatus, i.e. terminal A. The Narasimhalu patent (hereinafter '298) teaches a method and apparatus for controlling the dissimenation of digital information. [and] that the end user accesses the digital information with a tamper-proof controlled information access device."

09/221,479 ('683), Office Action, 11/12/99, p. 3-5 (IT00065799-801)

"With respect to the remaining issues, Applicants respectfully disagree. For example, the Examiner objects to the use of "environment" as indefinite and unclear. This word, however, is not used in isolation, but rather in the context of several longer phrases, all of which are defined in the specification. The phrase "protected processing environment," for example, is used in Claims 11 and 15-18 and described on at least, for example, pages 7-8 and 25 of the specification. The term "virtual

Claim Term	MS Construction
	distribution environment" used in Claim 11 is described, for example, on page 7 of the specification. The terms are also described in the commonly copending application Serial Number 08/388,107 of Ginter et al., filed 13 February 1995, entitled "System and Methods for Secure Transaction Management and Electronic Rights Protection." A copy of the incorporated Ginter application can be provided to the Examiner upon request." (pages 7, 7-8 and 25 of the original specification are '721 2:62-3:13, 2:62-3:34 and 8:6-28 of the issued patent)

"The role of go-between 4700 may, in some circumstances, be played by one of the participant's SPU's 500 (PPEs), since SPU (PPE) behavior is not under the user's control, but rather can be under the control of rules and controls provided by one or more other parties other than the user (although in many instances the user can contribute his or her own controls to operate in combination with controls contributed by other parties)." ('683 24:26)

08/689,754 ('721), Amendment, 04/14/99, p. 13

Extrinsic:

Processing: 1. The performance of logical operations and calculations on datum including temporary retention of data in processor storage while the data is being operated on.(IBM)

Environment: 1. The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system. 2. In computer security, those factors, both internal and external, of an ADP system that help to define the risks associated with its operation (Longley)

- IT used "tm" symbol with "Protected Processing Environment" (Panel Abstract: The InterTrust Commerce Architecture, presented at 20th NISSC, 1997)

Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment*. (ITG, 8/21/95, IT00032375, TD00068B)

Protected Processing Environment (PPE) technology: The InterTrust technology that provides the protected software environment within the InterRights Point. Protected Processing Environment technology is responsible for the encryption/decryption of data, protected processing of DigiBox containers, and other secure operations, such as protected database access. (ITG, 1997-1998, ML00012B)

Protected Processing Environment (PPE): The PPE is the secure part of a VDE node: either a hardware or software-protected environment in which VDE mechanisms run without external interference. There are various PPE realizations (e.g., physically protected hardware) appropriate to different operational requirements (ITG, 3/7/1995, IT00709619, see footnote 2)

Secure Processing Unit: The physically secure hardware component of the SPE: a processor with local memory and non-volatile storage. The SPE consists of the SPU itself and the SPE software running on the SPU. (ITG, 3/7/1995, IT00709620, see footnote 2)

"Protected Processing Environment (PPE): An InterTrust *node* has a unique *node ID* and contains a *Protected Processing Environment (PPE)* which performs *operations* on *containers* and *control structures* under rules specified by *PERCs* and which may be realized in a tamper resistant hardware component or in tamper-resistant software and a *protected database*, which stores *control objects* and *InterTrust applications*, operating outside the *PPE*, which manipulate *content* and *control objects* through requests to the *PPE*" (ITG, 4/06/95, IT00028206)

"All the terms in italics have specific definitions (in the glossary) with respect to InterTrust." 950406: *Global replace of "VDE" with "InterTrust" to match new terminology.* (ITG, 4/06/95, IT00028206)

Protected Environment: A portion of the node software that uses, and protects, the protected node data |

Claim Term	MS Construction
	such as cryptographic keys. The protected environment is responsible for performing all the protected functions for manipulating containers and content; that is, all the operations governed by controls. (ITG, 5/12/95, IT00028294) Protected Processing Environment: (alternate definition): The protected environment in which the cryptographic and control functions of InterTrust run. The PPE may be protected environmentally (e.g., as a physically protected server machine) or may employ software-based tamper resistance techniques. (ITG, 8/21/95, IT00032377, TD00068B) Secure Processing Environment (SPE): A hardware-supported realization of the PPE, protected from tampering by physical security techniques. No longer preferred because of the potential confusion between the "S" in the acronym and "S" as in "Software" (which this isn't). [REPLACEMENT UNCERTAIN] (ITG, 5/12/95, IT00028302) Protected Processing Environment (PPE): The InterTrust protected software environment within the InterTrust Commerce Node. The PPE is responsible for the encryption/decryption of data, protected processing of DigiBox containers, and other secure operations, such as database access. (ITG, 11/17/96, IT00035871, TD00189J)
protecting 683.2	Intrinsic: - VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users." ('193 4:51-56) - "An attacker would gain little benefit from intercepting this information since it is transmitted in protected form; she would have to compromise electronic appliance 600(1) or 600(N) (or the SPU 500(1), 500(N)) in order to access this information in unprotected form." ('193 228:25) - Even if the object is stored locally to the VDE node, it may be stored as a secure or protected object so that it is not directly accessible to a calling process. ('193 192:14-17) - ('193 228:25-30); ('193 6:33-35); ('193 15:41-46); ('193 17:22-28) Extrinsic: Hoffman, Modern Methods for Computer Security & Privacy at 134 Dictionary of Computing, 3rd Ed. (1990) ("Protected Location: A memory location that can only be accessed by an authorized user or process."; "Protected domain: A set of access privileges to protected resources.") Webster's New World Dictionary of Computer Terms, 4th Ed. (1992) ("To prevent unauthorized access to programs or a computer system; to shield against harm.") The New IEEE Standard Dictionary of Electrical and Electronics Terms, 5th Ed. (1993) ("Protection: (1) (computing systems). See: Storage protection (2) (software). An arrangement for restricting access to or use of a all, or part, of a computer system." ; "Storage protection: An arrangement for preventing access to storage for either reading or writing, or both.") IN00862862 Security: The combination of integrity and secrecy, applied to data. (ITG, 5/12/95, IT00028295) Secrecy: The inability to obtain any information from data. (ITG, 5/12/95, IT00028294)
record (n.) 912.8, 912.35	Intrinsic: "The selected method event record 1012, in turn, specifies the appropriate information (e.g., load module(s) 1100, data element UDE(s) and MDE(s) 1200, 1202, and/or PERC(s) 808) used to construct

Claim Term	MS Construction
	a component assembly 690 for execution in response to the event that has occurred. ..." ('193 138:12-47) Extrinsic: Record: 1. In programming languages, an aggregate that consists of data objects, possibly with different attributes, that usually have identifiers attached to them. In some programming languages, records are call structures. 2. A set of data treated as a unit. 3. A set of one or more related data items grouped for processing. (IBM) Record: 1. In computing, a collection of related data treated as a unit, e.g. details of name, address, age, occupation and department of an employee in a personnel file. 2.. In computing, to store signals on a recording medium for later use..(Longley) New IEEE Standard Dictionary of Electrical and Electronics Terms (5ᵗʰ ed. 1993)
required 912.8, 861.58	Intrinsic: See "allow." Extrinsic:
resource processed 891.1	Intrinsic: - ('193 72:39-44); ('193 75:15-30); ('193 283:23-28) "Smart objects may have the means to request use of one or more services and/or resources. Services include locating other services and/or resources such as information resources, language or format translation, processing, credit (or additional credit) authorization, etc. Resources include reference databases, networks, high powered or specialized computing resources (the smart object may carry information to another computer to be efficiently processed and then return the information to the sending VDE installation), remote object repositories, etc. Smart objects can make efficient use of remote resources (e.g. centralized databases, super computers, etc.) while providing a secure means for charging users based on information and/or resources actually used." ('193 38:60-39:8) Extrinsic: Resource: 1. Any of the data processing system elements needed to perform required operations, including storage, input/output units, one or more processing units, data, files, and programs. 2. Any facility of a computing system or operating system required by a job or task, and including main storage, input/output devices, processing unit, data sets, and control or processing programs.(IBM) Processed: 1. The performance of logical operations and calculations on datum including temporary retention of data in processor storage while the data is being operated on. (IBM) Process: (1) in computing, the active system entity through which programs run. The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system. 2. In computing, a program in execution. (4) In computing, a program is a static piece of code and a process is the execution of that code. (Longley)
rule 861.58, 683.2	Intrinsic: - "A system as in claim 17, said memory further storing at least one rule associated with said first secure container, said first secure container rule at least in part governing at least one aspect of access to or use of said governed item. A system as in claim 19, said at least first secure container rule further including a second rule at least

Claim Term	MS Construction
	in part restricting the number of accesses and/or uses a user may make of said governed item."

09/221,479('683), Preliminary Amendment, 12/28/99, p. 5 (IT00065690)

"Claims 7-11, ... are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (5,412,717) in view of Narasimhalu et al (5,499,298). Fischer discloses a method and apparatus including a system monitor which limits the ability of a program about to be executed to the use of predefined resources, ... The set of authorities and restrictions are referred to as "program authorization information" or "PAI". ... A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. ... memory containing a first rule corresponds to a first PAI under a first PCB ... ... Here, Fischer provides a secure container in the form of a program, i.e. a governed item, having an associated PAI, i.e. at least one rule associated with the secure container."

09/221,479 ('683), Office Action, 11/12/99, p. 3-4 (IT00065799-800)

- In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed. ('193 6:24-30)
- "at least one rule and/or control associated with the software agent that governs the agent's operation." ('193 241:2-3)

- "FIG. 4 illustrates examples of some different types of rules and/or control information" ('683 11:37-38)
- "If necessary, trusted go-between 4700 may obtain and register any methods, rules and/or controls it needs to use or manipulate the object 300 and/or its contents (FIG. 122 block 4778)." ('683 47:40-45)
- "In this further user interaction provided by object submittal manager 774, the user may specify permissions, rules and/or control information to be applied to or associated with the new object 300." ('193 106:60)
- "at least one rule and/or control associated with the software agent that governs the agent's operation." ('193 241:2)
- "The usage-related "rules and controls" may, for example, specify what a user can and can't do with the content and how much it costs to use the content." ('193 55:46-49)
- "Container 300x is specified as a content object that is empty of content. It contains a control set that contains the following rules:

    1. A write_without_billing event that specifies a meter and a general budget that limits the value of writing to $15.00.

    2. Audits of usage are required and will be stored in object 300w under control information specified in that object.

    3. An empty use control set that may be filled in by the owner of the information using predefined methods (method options)." ('193 243:35-37)

- "an object creator or other provider can specify within a descriptive data structure 200, certain rules, integrity constraints and/or other characteristics that can or should be applied to the object after it has been imported into a target rights management environment." ('861 17:49-53)

- ('683 54:29-37); ('193 56:28-35); ('193 53:60-63); ('683 47:40-45)

Extrinsic:

Rule: In computing, a statement in an expert system that enables the likelihood of an assertion, or the value of an object, to be established. A rule combines lower level assertions or objects to produce a value for a higher level assertion or object. (Longley)

See Business Rule: A specification of the conditions governing how content and controls in DigiBox containers may be manipulated. A business rule may specify pricing, terms of use terms, operational

Claim Term	MS Construction
	restrictions, payment methods, and other aspects of information use. A rule may also specify consequences related to usage reporting and payment, for example, specifying that each purchase of content must be reported to its creator. (ITG, 11/17/96, IT00035863, TD00189J) "Rules and Controls" means any electronic information that directs, enables, specifies, describes, and/or provides contributing means for performing or not-performing, permitted and/or required operations related to Content, including, for example, restricting or otherwise governing the performance of operations, such as, for example, Management of such Content. (License Agreement: IT and Universal Music Group, 4/13/99, Exhibit 11 to InterTrust 30(b)(6)) Que at 348; Webster's New World Dictionary of Computer Terms (4th ed.) at 365
secure 193.1, 193.11, 193.15, 912.35, 861.58, 891.1, 683.2, 721.34	Intrinsic: Because this term is indefinite and used inconsistently, each use of "secure" and forms thereof in the asserted patents is relevant and herein included by reference. The following examples are illustrative. - "HPEs 655 may be provided in two types: secure and not secure." ('193 80:8-9) - "Because secondary storage 652 is not secure, SPE 503 must encrypt and cryptographically seal (e.g., using a one-way hash function initialized with a secret value known only inside the SPU 500) each swap block before it writes it to secondary storage." ('193 107:39-42) - "Insecure external memory may reduce the wait time for swapped pages to be loaded into SPU 500, but will still incur substantial encryption/decryption penalty for each page." ('193 125:56-59) - "The following is a non-exhaustive list of some of the advantageous features provided by ROS 602 in the preferred embodiment: ... Secure secure communications secure control functions secure virtual memory management information control structures protected from exposure data elements are validated, correlated and access controlled components are encrypted and validated independently components are tightly correlated to prevent unauthorized use of elements control structures and secured executables are validated prior to use to protect against tampering integrates security considerations at the I/O level provides on-the-fly decryption of information at release time enables a secure commercial transaction network flexible key management features" ('193 72:52, 73:19) - "ROS 602 generates component assemblies 690 in a secure matter. As shown graphically, in FIGS. 111 and 11J, the different elements comprising a component assembly 690 may be "interlocking" in the sense that they can only go together in ways that are intended by the VDE participants who created the elements and/or specified the component assemblies. ROS 602 includes security protections that can prevent an unauthorized person from modifying elements, and also prevent an unauthorized person from substituting elements." (82:60) - - "Because of VDE security, including use of effective encryption, authentication , digital signature, and secure database structures, the records contain within a VDE card arrangement may be accepted as valid transaction records for government and/or corporate recordkeeping requirements." (19:49) - "In order to maintain security, SPE 503 must encrypt and cryptographically seal each block being swapped out to a storage device external to a supporting SPU 500, and must similarly decrypt, verify the cryptographic seal for, and validate each block as it swapped into SPU 500." (123:60) - "As mentioned above, memory external to SPU 500 may not be secure. Therefore, when security is required, SPU 500 must encrypt secure information before writing it to external memory before using it." (69:29) - "Only those processes that execute completely within SPEs 503 (and in some cases, HPEs 655) may be considered to be truly secure. Memory and other resources external to SPE 503 and HPEs 655 used

Claim Term	MS Construction
	to store and/or process code and/or data to be used in secure processes should only receive and handle that information in encrypted form unless SPE 503/HPE 655 can protect secure process code and/or data form non-secure processes." (79:11) - "From time to time, two parties (e.g., PPEs A and B), will need to establish a communication channel that is know by both parties to be secure form eavesdropping, secure from tampering, and to be in use solely by the two parties whose identifies are correctly known to each other." (215:35) - "Since all secure communications are at least in part encrypted and the processing inside the secure subsystem is concealed form outside observation and interference, the present invention ensures that content control information can be enforced." ('193 46:4-8) '193 199:38-47, 221:1-21 See also prior art referenced in the relevant file histories, e.g. Stefik; Tygar et al., "Dyad: A System for Using Physically Secure Coprocessors," School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213 (May 1991). Extrinsic: "No data system can be made secure without physical protection of some part of the equipment." (Davies, p. 3)[9] "Security is a negative attribute. We judge a system to be secure if we have not been able to design a method of misusing it which gives some advantage to the attacker." (Davies, p.4) "Various criteria exist for secure systems - U.S. Dept. of Defense Trusted Computer Security Evaluation Criteria (TCSEC), the Orange Book, Red Book, European and Canadian guidelines, U.S. National Institute of Standards and Technology, and United Kingdom guidelines." (Neumann)[10] "Security: 1. Protection against unwanted behavior. In present usage, computer security includes properties such as confidentiality, integrity, availability, prevention of denial of service and prevention of generalized misuse. 2. The property that a particular security policy is enforced, with some degree of assurance. 3. Security is sometimes used in the restricted sense of confidentiality, particularly in the case of multilevel security. Multilevel Security - A confidentiality policy based on the relative ordering of multilevel security labels (really multilevel confidentiality, ex. - no adverse flow of information with respect to sensitivity of information)" (Neumann, Glossary) "There are two principal objectives: secrecy (or privacy), to prevent unauthorized disclosure of data; and authenticity or integrity) [sic], to prevent the unauthorized modification of data. ... Note, however, that whereas it can be used to detect message modification, it cannot prevent it. Encryption alone does not protect against replay, because an opponent could simply replay previous ciphertext." (Denning, p.5) "A cipher in unconditionally secure if, no matter how much ciphertext is intercepted, there is not enough information in the ciphertext to determine the plaintext uniquely." (Denning, p.5) (Davies, p. 41, 380) "A cipher is computationally secure, or strong, if it cannot be broken by systematic analysis with available resources." (Denning, p.5) (Davies, p.41, 370) Security: The combination of integrity and secrecy, applied to data. (ITG, 5/12/95, IT00028295) Secrecy: The inability to obtain any information from data. (ITG, 5/12/95, IT00028294) ". . . security includes concealment, integrity of messages, authentication of one communicating party by the other. . ." (Neumann, p. 8)

---

[9] "Davies" herein refers to Davies, D., et al, Security for Computer Networks, 1984.
[10] "Neumann" herein refers to Neumann, P.G., Computer Related Risks, 1995

Claim Term	MS Construction
	"Computer security rests on confidentiality, integrity, and availability. The interpretations of these three aspects vary, as do the contexts in which they arise.

Confidentiality is the concealment of information or resources. [] Confidentiality also applies to the existence of data, which is sometimes more revealing than the data itself.

[] All mechanisms that enforce confidentiality require supporting services from the system. The assumption is that the security services can rely on the kernel, and other agents, to supply correct data. Thus, assumptions and trust underlie the confidentiality mechanisms.

Integrity refers to the trustworthyness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the informationz) and origin integrity (the source of the data, often called authentication).

Integrity mechanisms fall into two classes: prevention mechanisms and detection mechanisms.

Protection mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways.

Detection mechanisms do not try to prevent violations of integrity; they simple report that the data's integrity in no longer trustworthy." (Bishop, p. 4-6)[11]

"Definition 4-1. A security policy is a statement that partitions the states of the system into a set of authorized, or secure, states and a set of unauthorized, or nonsecure, states.

Definition 4-2. A secure system is a system that starts in an authorized state and cannot enter an unauthorized state." (Bishop, p. 95)

"24.5.1 Secure Systems
Systems designed with security in mind have auditing mechanisms integrated with the system design and implementation." (Bishop, p.706)

"Computer security is assuring the secrecy, integrity, and availability of components of computing systems. The three principal pieces of a computing system subject attacks are hardware, software, and data. These three pieces, and the communications between them, constitute the basis of computer security vulnerabilities. This chapter has identified four kinds of attacks on computing systems: interruptions, interceptions, modifications, and fabrications.

Three principles affect the direction of work in computer security. By the principle of easiest penetration, a computing system penetrator will use whatever means of attack is the easiest; therefore. All aspects of computing system security need to be considered at once. By principle of timeliness, a system needs to be protected against penetration only long enough so that penetration is of no value to the penetrator. The principle of effectiveness states that controls must be usable and used in order to serve purpose.

Controls can be applied at the levels of data, programs, the system, physical devices, communications links, the environment, and personnel. Sometimes several controls are needed to cover a single vulnerability, and sometimes one control addresses several problems at once." (Pfleeger, p.4)

See also InterTrust's Rule 30(b)(6) testimony and Microsoft PLR 4-2 Exhs. E & F as revised. (Examples follow). Webster's New 20th century Dictionary (1947) at 1540-41); Pfleeger at 4-5; Spencer, Personal Computer Dictionary at 156; The Computer Glossary at 460; McGraw-Hill Dictionary of Scientific and Technical Terms at 1788; Practical Unix Security at 11-12 (O'Reilly 1991); Bishop, Computer Security (2002) pp. 3-24, 47; Hoffman, Modern Methods for Computer Security and Privacy at 2, 134-35; Mullender, ed., Distributed Systems (Addison Wesley 2d ed.) at 367, 420; Landewehr, "Formal Models for Computer Security" (ACM 1981); Merkle, "Protocols for Public Key Cryptosystems" (IEEE 1980); Cooper, Computer & Communication Security, at 383; Baker, The Computer Security Handbook at 273; Computer Security Handbook at 389; Matheson et al., Robustness and Security of Digital Watermarks;

[11] ``Bishop'' herein refers to ``Bishop, M., Computer Security, Art & Science, 2003).

Claim Term	MS Construction
	National Information Systems Security (INFOSEC) Glossary at 49-50; Internet Security Glossary (RFC2828); Tanenbaum, Modern Operating Systems (1992) at 181-82
	IN64706-45, IN176319-72, IT735936 (integrity), IT735938-9
	IN00862862, IT1678-96, IT39208-26, IT702969-83, IT399877-80
	"Secure. Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user."; "Computer Security. 1. Concepts, techniques, technical measures, and administrative measures used to protect the hardware, software and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification or use or loss. 2. Protection resulting from the application of computer security." (IBM)
	"Security: Freedom from risk or danger. Safety and assurance of safety"; "secure state - a condition in which none of the subjects in a system can access objects in an unauthorized manner..."(Russell, Computer Security Basics, 1992, pp. 8-11, 113, 227, 420)
	"Various criteria exist for secure systems - U.S. Dept. of Defense Trusted Computer Security Evaluation Criteria (TCSEC), the Orange Book, Red Book, European and Canadian guidelines, U.S. National Institute of Standards and Technology, and United Kingdom guidelines."
	The New IEEE Standard Dictionary of Electrical and Electronics Terms, 5th Ed. (1993) at 1181 ("The protection of computer hardware and software from accidental or malicious access, use, modification, destruction, or disclosure.")
	Dictionary of Computing, 3rd Ed. (1990) at 406 ("Prevention of or protection against (a) access to information by unauthorized recipients or (b) intentional but unauthorized destruction or alteration of that information.")
	Information Security Dictionary of Concepts, Standards, and Terms (1992) ("The quality or state of being cost-effectively protected from undue losses (e.g. loss of goodwill, monetary loss, loss of ability to continue operations, etc.)")

secure container
 	
912.35, 861.58, 683.2
	See "secure" and "container"
	
	Intrinsic:
	
	- Prosecution History of '861 Patent:
	  "Anderson [U.S. Patent No. 5,537,526] does not explicitly address a secure container *per se*, but does place documents into containers [Fig. 8 202] and place restriction via links attached to documents ... which can include restrictions ... Such security tools are rightfully attached to a structure encapsulating the document, e.g. its container."
	  08/805,804 ('861), Office Action, 06/25/98, p. 5. MSI 27417-25
	- Prosecution History of '683 Patent:
	  "Claims 7-11, ... are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (5,412,717) in view of Narasimhalu et al (5,499,298). ... The set of authorities and restrictions are referred to as "program authorization information" or "PAI". ... A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. ... Here, Fischer provides a secure container in the form of a program, i.e. a governed item, having an associated PAI, i.e. at least one rule associated with the secure container."
	  09/221,479('683), Office Action, 11/12/99, p. 3-4 (IT00065799-800 in IT65863-65)
	- Prosecution History of Application 08/689,606, filed 12 August 1996: (issued as USP 5,943,422 incorporating '107) Amendment dated 2 July 1998:
	  "1. (Amended) A rights management method comprising: (a) receiving an information signal; (b) steganographically decoding the received information signal to recover digital rights management control information packaged within at least one secure digital container; and (c) performing at least one rights management operation based at least in

Claim Term	MS Construction
	part on the recovered digital rights management control information. [] Remarks [] For example, amended Claims 1, 15 and 22 each recite a digital secure container in combination. Neither Rhoads [USP 5,636,292], nor any of the other applied references, teaches or suggests the recited combination of features including any digital secure container." - Rhoads, USP 5,636,292: "Fully Exact Steganography Prior art steganographic methods currently known to the inventor generally involve fully deterministic or "exact" prescriptions for passing a message. Another way to say this is that it is a basic assumption that for a given message to be passed correctly in its entirety, the receiver of the information needs to receive the exact digital data file sent by the sender, tolerating no bit errors or "loss" of data. By definition, "lossy" compression and decompression on empirical signals defeat such steganographic methods. (Prior art, such as the previously noted Komatsu work, are the exceptions here.) The principles of this invention can also be utilized as an exact form of steganography proper. It is suggested that such exact forms of steganography, whether those of prior art or those of this invention, be combined with the relatively recent art of the "digital signature" and/or the DSS (digital signature standard) in such a way that a receiver of a given empirical data file can first verify that not one single bit of information has been altered in the received file, and thus verify that the contained exact steganographic message has not been altered. " (55:5-26) "One exemplary application is placement of identification recognition units directly within modestly priced home audio and video instrumentation (such as a TV). Such recognition units would typically monitor 'audio and/or video looking for these copyright identification codes, and thence triggering simple decisions based on the findings, such as disabling or enabling recording capabilities, or incrementing program specific billing meters which are transmitted back to a central audio/video service provider and placed onto monthly invoices." (29:23) - "Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility." ('683 8:50-52) - "Even if the object is stored locally to the VDE node, it may be stored as a secure or protected object so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security requisites needed to access the object." ('193 192:41-) - "Electronic delivery person 4060 receives item 4054 in digital form and places it into a secure electronic container 302--thus forming a digital "object" 300. A digital object 300 may in this case be, for example, as shown in FIGS. 5A and 5B, and may include one or more containers 302 containing item 4054. FIG. 88 illustrates secure electronic container 302 as an attaché case handcuffed to the secure delivery person's wrist. Once again, container is shown as a physical thing for purposes of illustration only--in the example it is preferably electronic rather than physical, and comprises digital information having a well-defined structure (see FIG. 5A). Special mathematical techniques known as "cryptography" can be used to make electronic container 302 secure so that only intended recipient 4056 can open the container and access the electronic document (or other item) 4054 it contains." ('683 15:56-16:6) - "Because container 152 can only be opened within a secure protected processing environment 154 that is part of the virtual distribution environment described in the above-referenced Ginter et al. patent disclosure" ('712 168:22-25) - "A VDE content container is an object that contains both content (for example, commercially distributed electronic information products such as computer software programs, movies, electronic publications or reference materials, etc.) and certain control information related to the use of the object's content." ('193 19:15-21) - ('193 82:24-45); ('193 192:36-52); ('683 18:49-56);('861 4:51-64) Extrinsic: Container: VDE objects are represented in a special form called a container. The container is

Claim Term	MS Construction
	implemented within the VDE as an object-oriented container class. The container class provides a standard method by which applications software may encapsulate and read information stored within the object. Additionally, the container may include procedural information associated with the data being stored. Containers may be nested, and share attributes with nested elements. Nested containers are stored within a larger container. VDE recognizes the presence of additional objects within the content, and allows the nested containers to share, extend or override the attributes of an outer container. (VDE ROI DEVICE v1.0a 9 Feb 1994, IT00008572) Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Container: In data security, a multilevel information structure. A container has a classification and may contain objects and/or other containers. (Longley) Container: A protected (encrypted) storage object that incorporates descriptive information, protected content, and (optionally) control objects applicable to that content. (ITG, 3/7/1995, IT00709617, see footnote 2) Container: A contains protected *content*, which is divided into one or more *atomic elements*, and, optionally, *PERCs* governing the *content* and may be manipulated only as specified by a *PERC*. (ITG, 4/6/95, IT00028206, see footnote 5) Container: A packaging mechanism, consisting of: *One or more Element-derived components. *An organization mechanism which provides a unique name within a flat namespace for each of the components in a Container (ITG, 5/12/95, IT00028293) Container: A protected digital information storage and transport mechanism for packaging content and control information. (ITG, 8/21/95, IT00032372, TD00068B) "Secure Container(s)" means electronic container(s) or electronic data arrangements that: (I) use one or more cryptographic or other obfuscation techniques to provide protection for at least a portion of the Content thereof; and (ii) supports the use of Rules and Controls to enable the Management of Content. (License Agreement IT and Universal Music Group, 4/13/99, Exhibit 11 to IT 30(b)(6)) A protected digital information storage and transport mechanism for packaging content and control information. (IT 691187) Secure container: A DigiBox container provides security through encryption and the PPE of a commerce node. A secure container does not require a secure communications transport mode. (IT 35965) A DigiBox container provides for the persistent protection of its properties. (IT 35920) DigiBox containers ensure integrity. (IT 35895)
secure container governed item 683.2	Intrinsic: Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Container: In data security, a multilevel information structure. A container has a classification and may contain objects and/or other containers. (Longley) Item: 1. An element of a set of data. 2. One unit of a commodity such as one ox, one bag, or one can. (IBM) Item: In computing, a group of related characters treated as a unit. For example, a record may comprise a number of items, that in turn may consist of other items. (Longley) Container: A protected (encrypted) storage object that incorporates descriptive information, protected content, and (optionally) control objects applicable to that content. (ITG, 3/7/95, IT00709617, see footnote 2) Container: A packaging mechanism, consisting of: *One or more Element-derived components. *An

Claim Term	MS Construction
	organization mechanism which provides a unique name within a flat namespace for each of the components in a Container (ITG, 5/12/95, IT00028293)

Container: A protected digital information storage and transport mechanism for packaging content and control information. (ITG, 8/21/95, IT00032372, TD00068B)

Secure Processing Unit: The physically secure hardware component of the SPE: a processor with local memory and non-volatile storage. The SPE consists of the SPU itself and the SPE software running on the SPU. (ITG, 3/7/95, IT00709620, see footnote 2)

DigiBox Container: InterTrust's secure cryptographic data structure for packaging and containing contents and controls. A DigiBox container provides for the persistent protection of its content and controls through the Protected Processing Environment of XECutor. A DigiBox container eliminates the need for a secure communications channel, such as SSL or SHTTP. (ITG, 10/2/96, IT00035893, TD00189F)

DigiBox Container: A format for protected storage and transport of digital content and business rules. The DigiBox container uses cryptography to ensure that the information it holds is protected and can only be manipulated by InterTrust Commerce Nodes. (ITG, 11/17/96, IT00035866, TD00189J) |
| secure database

193.1, 193.11, 193.15 | Intrinsic:

- See '193, Figures 7, 10.

- "FIG. 36 shows an example of how a new record or element may be inserted into a secure database 610. The load process 1070 shown in FIG. 35 checks each data element or item as it is loaded to ensure that it has not been tampered with, replaced or substituted. In the process 1070 shown in FIG. 35, the first step that is performed is to check to see if the current user of electronic appliance 600 is authorized to insert the item into secure database 610 (block 1072)... The non-secure element within its security wrapper may then be stored within secure databases 610."

- "The keys to decrypt secure database 610 records are, in the preferred embodiment, maintained solely within the protected memory of an SPU 500."

- "By using this process, SPE 503 can protect the data structure (including the indexes) of secure databases 610 against substitutions of old items and against substitution of indexes for current items."

- "The security of secure databases 610 files may be further improved by segmenting the records into "compartments." Different encryption/decryption keys may be used to protect different "compartment." This strategy can be used to limit the amount of information within secure database 310 that is encrypted with a single key/ Another technique for increasing secure database 610 may be to encrypt different portions of the same records with different keys so that more than one key may needed to decrypt these records."

- "Each electronic appliance 600 may have an instance of secure database 610 that securely maintains the VDE items. FIG. 16 shows one example of a secure database 610.

- "VDE Secure Database 610: VDE 100 stores separately deliverable VDE elements in a secure (e.g., encrypted) database 610 distributed to each VDE electronic appliance 610. The database 610 in the preferred embodiment may store and/or manage three basic classes of VDE items: VDE objects, VDE process elements, and VDE data structures."

- "Secure Database Keys: PPE 650 preferably generates these secure database keys and never exposes the outside of the PPE. They are site-specific in the preferred embodiment, and may be "aged" as described above. As described above, each time an updated record is written to secure database 610, a new key may be used and kept in a key list within the PPE." (212:36)

- "Secure database encryption keys in the preferred embodiment are frequently changing and are also site specific." (219:30)

- ('193 79:24); ('193 71:28-40); ('193 111:59-67) |

Claim Term	MS Construction
	Extrinsic: Secure store: The Secure store is the system area that provides an encrypted storage method for storing ROI internal files and other highly secure information. In some applications, entire media volumes can be distributed encrypted as part of the secure store to enhance overall security for the content by obscuring the file system and media descriptors associated with the volume. A dedicated volume or partition will only be required if an application cannot be supported without it. (e.g. a required government security level for the specific application). In most cases, the user will not be required to dedicate an entire volume or partition of the hard disk, and the secure store will be supported using an encrypted file, or files, on the hard disk. ROI will also support a dedicated partition as an option to the administrator of a network server, as one of several ways to assure the integrity of the system. (VDE ROI DEVICE v1.0a 9 Feb 1994, IT00008586) Database: 1. A collection of data with a given structure for accepting, storing, and providing, on demand, data for multiple users. 2. A collection of interrelated data organized according to a database schema to serve one or more applications. 3. A collection of data fundamental to a system. 4. A collection of data fundamental to an enterprise.(IBM) Database: 1. An extensive and comprehensive set of records collected and organized in a meaningful manner to serve a particular purpose. 2. In computing, a collection of stored operational data used by the applications system of an enterprise. (Longley) "The basic security requirements of data base systems are not unlike the security requirements of other computing systems we have studied. The basic problem-access control, exclusion of spurious data, authentication of users, reliability-have appeared in many context so far in this book. Following is a list of requirements for security of data base systems. Physical data base integrity, so that the data of a data base is immune to physical problems, such as power failures, and so that it is possible to reconstruct that data base if it is destroyed through a catastrophe. Logical data base integrity, so that the structure of the data base is preserved. With logical integrity of a data base, a modification to the value of one field does not affect other field, for example. Element integrity, so that the data contained in each element is accurate. Auditability, to be able to track who has accessed (or modified) the elements in the data base. Access control, so that a user is allowed to access only authorized data and so that different user can be restricted to different modes of access (for example, read or write). User authentication, to be sure that every user is positively identified, both for audit trail and for permission to access data. Availability, meaning that users can access the data base in general and all the data for which they are authorized." (Pfleeger) Security: The combination of integrity and secrecy, applied to data. (ITG, 5/12/95, IT00028295) Secrecy: The inability to obtain any information from data. (ITG, 5/12/95, IT00028294)
secure execution space 721.34	Intrinsic: - Prosecution History of '721 Patent : "execution spaces" "refers to a resource which can be used for execution of a program or process." Amendment - - "Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. Tamper resistant barriers may be used to protect this programming or other conditioning. The assurance levels described below are a measure or assessment of the effectiveness with which this programming or other conditioning is

Claim Term	MS Construction
	protected." - ('721 3:16-23) - - "A protected processing environment or other secure execution space protects itself by executing only those load modules or other executables that have been digitally signed for its corresponding assurance level." - "Different protected processing environments (secure execution spaces) might examine different subsets of the multiple digital signatures--so that compromising one protected processing environment (secure execution space) will not compromise all of them." - "The internal ROM 532 and RAM 534 within SPU 500 provide a secure operating environment and execution space." ('193 69:33-35) - SPU 500 general purpose RAM 534 provides, among other things, secure execution space for secure processes. ('193 70:43-44) - "Virtual memory manager 580 provides a fully "virtual" memory system to increase the amount of "virtual" RAM available in the SPE secure execution space beyond the amount of physical RAM 534a provided by SPU 500." ('193 109:24-45) Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Execution: The process of carrying out an instruction or instructions of a computer program by a computer. (IBM) Space: 1. A site intended for storage of data. 2. A basic unit of area, usually the size of a singe character. 8. To cause a printer to move the paper a specified number of lines either before or after it prints a line. (IBM)
secure memory, memory 193.1, 193.11, 193.15	Intrinsic: - "Because secondary storage 652 is not secure, SPE 503 must encrypt and cryptographically seal (e.g., using a one-way hash function initialized with a secret value known only inside the SPU 500) each swap block before it writes it to secondary storage." ('193 107:39-46) - "Due to the practical limits on the amount of ROM 532 and RAM 534 that may be included within SPU 500, SPU 500 may store information in memory external to it, and move this information into and out of its secure internal memory space on an as needed basis." ('193 18:14-19); - "Such external memory may be used to store SPU programs, data and/or other information. For example, a VDE control program may be, at least in part, loaded into the memory and communicated to and decrypted within SPU 500 prior to execution. Such control programs may be re-encrypted and communicated back to external memory where they may be stored for later execution by SPU 500. "Kernel" programs and/or some or all of the non-kernel "load modules" may be stored by SPU 500 in memory external to it. Since a secure database 610 may be relatively large, SPU 500 can store some or all of secure database 610 in external memory and call portions into the SPU 500 as needed. As mentioned above, memory external to SPU 500 may not be secure. Therefore, when security is required, SPU 500 must encrypt secure information before writing it to external memory, and decrypt secure information read from external memory before using it. Inasmuch as the encryption layer relies on secure processes and information (e.g., encryption algorithms and keys) present within SPU 500, the encryption layer effectively "extends" the SPU security barrier 502 to protect information the SPU 500 stores in memory external to it." ('193 71:19-40) - "Key and Tag Manager 558 also provides services relating to tag generation and management. In the preferred embodiment, transaction and access tags are preferably stored by SPE 503 (HPE 655) in protected memory (e.g., within the NVRAM 534b of SPU 500). These tags may be generated by key and tag manager 558. They are used to, for example, check access rights to, validate and correlate data elements. For example, they may be used to ensure components of the secured data structures are not

Claim Term	MS Construction
	tampered with outside of the SPU 500." ('193 120:59-121:1) - "The degree of overall security of the VDE system is primarily dependent on the degree of tamper resistance and concealment of VDE control process execution and related data storage activities. Employing special purpose semiconductor packaging techniques can significantly contribute to the degree of security. Concealment and tamper-resistance in semiconductor memory (e.g., RAM, ROM, NVRAM) can be achieved, in part, by employing such memory within an SPU package, by encrypting data before it is sent to external memory (such as an external RAM package) and decrypting encrypted data within the CPU/RAM package before it is executed. This process is used for important VDE related data when such data is stored on unprotected media, for example, standard host storage, such as random access memory, mass storage, etc." ('193 21:26-40) - "Secondary storage 662 may comprise the same one or more non-secure secondary storage devices (such as a magnetic disk and a CD-ROM drive as one example) that electronic appliance 600 uses for general secondary storage functions. In some implementations, part or all of secondary storage 652 may comprise a secondary storage device(s) that is physically enclosed within a secure enclosure. However, since it may not be practical or cost-effective to physically secure secondary storage 652 in many implementations, secondary storage 652 may be used to store information in a secure manner by encrypting information before storing it in secondary storage 652. If information is encrypted before it is stored, physical access to secondary storage 652 or its contents does not readily reveal or compromise the information." ('193 62:43-58) - ('193 59:60-60:3); ('193 69:47-48); ('193 164:55-60); ('193 59:48-59); ('193 63:60-64:5); ('193 69:6-11); ('193 69:27-32); ('193 69:39-43); ('193 71:32-35); ('193 71:42-47); ('193 78:16-17); ('193 120:37-41) Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Memory: All of the addressable storage space in a processing unit and other internal storages that is used to execute instructions.(IBM)
secure operating environment, said operating environment 891.1	Intrinsic: - VDE provides a secure operating environment employing VDE foundation elements along with secure independently deliverable VDE components that enable electronic commerce models and relationships to develop." ('193 13:37-41) - "The internal ROM 532 and RAM 534 within SPU 500 provide a secure operating environment and execution space." (67:29) - ('193 34:26-49); ('193 72:52-73:37); ('193 77:30-44) Extrinsic: Execution environment: Some load modules contain code that executes in a ROI device. Some load modules will contain code that executes in the user's platform microprocessor. This allows methods to be constructed that execute in whichever environment is appropriate. For example an information method could be built to execute only in ROI secure space for government classes of security, or in the user's platform microprocessor for virtually all commercial applications. The public header of the load module will contain a field that indicates where it needs to execute. This functionality also allows for different ROI devices as well as different user platforms and allows methods to be constructed for either. It should be noted that load modules that execute outside of an ROI device are deemed insecure by the VDE Architecture and secure processes should not be implemented using load modules that execute outside of an ROI device. (VDE ROI DEVICE v1.0a, 9 Feb 1994, IT00008592) "Saltzer [SAL74] and Saltzer and Schroeder [SAL75] listed the following principles of the design of secure protection systems. Least privilege: Each user and each program should operate using the fewest privileges

Claim Term	MS Construction
	possible. In this way, the damage from an inadvertent or malicious attack is minimized. Economy of mechanism: The design of the protection system should be small, simple and straightforward. Such a protection can be exhaustively tested, perhaps verified, and trusted. Open design: The protection mechanism must not depend on the ignorance of potential attackers; the mechanism should be public, depending on secrecy of relatively few key items, such as a password table. An open design is also available for extensive public scrutiny. Complete mediation: Every access must be checked. Permission-based: The default condition should be denial of access. A conservative designer identifies those items that should be accessible, rather than those that should not. Separation of privilege: Ideally, access to objects should depend on more than one condition, such as user authentication plus a cryptographic key. In this way, someone who defeats one protection system will not have complete access. Least common mechanism: Shared objects provide potential channels for information flow. Systems employing physical or logical separation reduce the risk from sharing. Easy to use: If a mechanism is easy to use, it is unlikely to be avoided." (Pfleeger section 7.2) Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment*. (ITG, 8/21/95, IT00032375, TD00068B)
securely applying 891.1	Intrinsic: Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Applying: 1. In journaling, to place after-images of records into a physical file member. The after-images are recorded as entries in a journal. 2. An SMP process that moves distributed code and MVS-type programs to the system libraries. (IBM)
securely assembling 912.8, 912.35	Intrinsic: - ('193 87:33-40) - "ROS 602 also provides a tagging and sequencing scheme that may be used within the loadable component assemblies 690 to detect tampering by substitution. ('193 87:41-62) - "ROS 602 generates component assemblies 690 in a secure manner. As shown graphically in FIGS. 11I and 11J, the different elements comprising a component assembly 690 may be "interlocking" in the sense that they can only go together in ways that are intended by the VDE participants who created the elements and/or specified the component assemblies. ROS 602 includes security protections that can prevent an unauthorized person from modifying elements, and also prevent an unauthorized person from substituting elements." ('193 84:60-85:2) - "ROS 602 assembles these elements together into an executable component assembly 690 prior to loading and executing the component assembly (e.g., in a secure operating environment such as SPE 503 and/or HPE 655). ROS 602 provides an element identification and referencing mechanism that includes information necessary to automatically assemble elements into a component assembly 690 in a secure manner prior to, and/or during, execution." ('193 83:44-52) - ('107 page 782 claim 80); ('193 116:25-35); ('193 116:29-33) Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM)

Claim Term	MS Construction
securely processing 891.1	Intrinsic: - "VDE can satisfy the requirements of widely differing electronic commerce and data security applications by, in part, employing this general purpose transaction management foundation to securely process VDE transaction related control methods." ('193 25:52-57) - "For example, they [HPE and SPE] may each perform secure processing based on one or more VDE component assemblies 690, and they may each offer secure processing services to OS kernel 680." ('193 79:43-46) - "VDE methods 1000 are designed to provide a very flexible and highly modular approach to secure processing." ('193 181:18-19) - "In these cases, secure processing steps performed by an SPU typically must be segmented into small, securely packaged elements that may be "paged in" and "paged out" of the limited available internal memory space." (67:39) - ('193 21:43-22:31); ('193 109:24-45); ('193 139:28-31); ('683 24:26-33) - Load modules are not necessarily directly governed by PERCs 808 that control them, nor must they contain any time/date information or expiration dates. The only control consideration is the preferred embodiment is that one or more methods 1000 reference them using a correlation tag (the value of a protected object created by the load module's owner, distributed to authorized parties for inclusion in their methods, and to which access and use is controlled by one or more PERCs 808). If a method core 1000' references a load module 1100 and asserts the proper correlation tag (and the load module satisfies the internal tamper checks for the SPE 503), then the load module can be loaded and executed, or it can be acquired from, shipped to, updated, or deleted by, other systems. - ROS 602 also provides a tagging and sequencing scheme that may be used within loadable component assemblies 690to detect tampering by substitution. Each element comprising a component assembly 690 may be loaded into a SPU 500, decrypted using encrypt/decrypt engine 522, and then tested/compared to ensure that the proper element has been loaded. ...In addition, a validation/correlation tag stored under the encrypted layer of the loadable element may be compared to make sure it matches on or more tags provided by a requesting process. This prevents unauthorized use of information. As a third protection, a device assigned tag (e.g., a sequence number) stored under an encryption layer of loadable element may be checked to make sure it matches a corresponding tag value expected by SPU 500. This prevents substitution of older elements. Validation/correlation tags are typically passed only in secure wrappers to prevent plaintext exposure of this information outside of SPU 500.. - Key and Tag Manager 558 also provides service relating to tag generation and management. In the preferred embodiment, transaction and access tags are preferably stored by SPE 503 (HPE 665) in protected memory (e.g., within the NVRAM 534b of SPU 500). These tags may be generated by key and tag manager 558. They are used to, for example, check access rights to, validate and correlate data elements. For example, they may be used to ensure components of the secured data structures are not tampered with outside of the SPU 500. - Initiation of load module execution in this environment is strictly controlled by a combination of access tags, validation tags, encryption keys, digital signatures, and/or correlation tags. Thus, a load module 1100 may only be referenced if the caller knows it ID and asserts the shared secret correlation tag specific to that load module. The decrypting SPU may match the identification token an and local access tag of a load module after decryption. These techniques make the physical replacement of any load module 1100 detectable at the next physical access of a load module. - Meters and budgets are common examples of this. Expiration dates cannot be used effectively to prevent substitution of the previous copy of a budget UDE 1200. To secure these frequently updated items, a transaction tag is generated and included in the encrypted item each time that item is updated. A list of all VDE items Ids and the current transaction tags for each item is maintained as part of the secure database 610. UDEs 1200 are preferably encrypted using a site specific key once they are loaded into a site. This site-specific key marks a validation tag that may be derived from a cryptographically strong pseudo-random

Claim Term	MS Construction
	sequence by the SPE 503 and updated each time the record is written back to the secure database 610. This technique provided reasonable assurance that the UDE 1200 has not been tampered with nor submitted when it is requested by the system for the next use.
	Extrinsic:
	Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM)
	Process: 1. The performance of logical operations and calculations on datum including temporary retention of data in processor storage while the data is being operated on. (IBM)
	Process: Process: (1) in computing, the active system entity through which programs run. The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system. (2) In computing, a program in execution. . . .(4) In computing, a program is a static piece of code and a process is the execution of that code. (Longley)
	Processing: In legislation, as defined by the U.K. Data Protection Act o f 1984, pertaining to the amending, augmenting, deleting, or re-arranging of the data or extracting the information constituting the data and , in the case of personal data, processing means performing any of the abovementioned operations by reference to the data subject. (Longley)
securely receiving 891.1	Intrinsic:
	Prosecution History of Application 08/388,107: "Johnson's user database is not securely delivered, but rather is created at the license server by—and is under the control of—the site administrator."
	08/388,107, Amendment, 06/20/97, p. 23 (MS1028847)
	"[A]pplicants' independent claims ... require secure delivery of both first and second control items originating from someplace other than the appliance where they are used, at least in part, for controlling the same process, operation or the like. This feature in combination is not taught or suggested by Johnson and/or Rosen." (pg. 23)
	"Johnson's user database is not securely delivered, but rather is created at the license server by—and is under the control of—the site administrator." (pg. 23)
	"Rosen does not disclose or suggest securely delivering controls of plural different entities and/or appliances from at least one source remote to the receiving site or appliance as recited in applicants' independent claims ...., Rosen's is distinguishable at least because Rosen's merchant trusted agent (MTA) and customer trusted agent (CTA) are loaded into different appliances and operate in different appliances. ... Furthermore, such loading operation is performed at Rosen's physically secure device manufacturing site -- not from at least one source remote to the device." (pg. 23-24)
	08/388,107, Amendment, 06/20/97, p. 23, 23, 24 (MS1028847-48)
	- "Secure communications means employing authentication, digital signaturing, and encrypted transmissions." ('193 12:5-35, 12:33)
	- The appliance 600 may then open the secure electronic container ("attaché case") 302 and deliver the item it contains to recipient 4056 (FIG. 91B, block 4092D). ('683)
	- "FIGS. 114A-118 show example processes for securely receiving an item" ('683 14:64-65)
	- "By way of non-exhaustive summary, these present inventions provide a highly secure and trusted item delivery and agreement execution services providing the following features and functions:" ('683:6)
	- "When encrypted or otherwise secured information is delivered into a user's secure VDE processing area (e.g., PPE 650), a portion of this information can be used as a "tag" that is first decrypted or otherwise unsecured and then compared to an expected value to confirm that the information represents

Claim Term	MS Construction
	expected information. The tag thus can be used as a portion of process confirming the identity and correctness of received, VDE protected, information." (214:17) - "For objects in which maintaining security is particularly important, the permission records 808 and key blocks 810 will frequently be distributed electronically, using secure communications techniques (discussed below) that are controlled by the VDE nodes of the sender and receiver." ('193 129:8-13) - "Creator B ... may accept such a [new control] model if information associated with the one or more meter methods that record the number of bytes decrypted by users is securely packaged by distributor B's VDE secure subsystem and is securely, employing VDE communications techniques, sent to creator B in addition to distributor A" ('193 307:46-51) - ('193 209:27-30); ('193 29:64-30:4); ('193 36:29-33); ('193 45:39-45); ('193 153:53-67); ('193 293:4-7); ('683 15:67-16:4) Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Receiving: 1. To obtain and store data.(IBM) Secure Processing Unit: The physically secure hardware component of the SPE: a processor with local memory and non-volatile storage. The SPE consists of the SPU itself and the SPE software running on the SPU. (ITG, 3/7/1995, IT00709620, see footnote 2)
security level, level of security 721.1; 721.34, 912.8	Intrinsic: - ('193 21:26-31); ('193 45:52-59), but only as to 912.8. - "For example, protected processing environments or other secure execution spaces that are more impervious to tampering (such as those providing a higher degree of physical security) may use an assurance level that isolates it from protected processing environments or other secure execution spaces that are relatively more susceptible to tampering (such as those constructed solely by software executing on a general purpose digital computer in a non-secure location)." - "The present invention may use a verifying authority and the digital signatures it provides to compartmentalize the different electronic appliances depending on their level of security (e.g., work factor or relative tamper resistance)." - "Assurance level I might be used for an electronic appliance(s) 61 whose protected processing environment 108 is based on software techniques that may be somewhat resistant to tampering. An example of an assurance level I electronic appliance 61A might be a general purpose personal computer that executes software to create protected processing environment 108. An assurance level II electronic appliance 61B may provide a protected processing environment 108 based on a hybrid of software security techniques and hardware-based security techniques. An example of an assurance level II electronic appliance 61B might be a general purpose personal computer equipped with a hardware integrated circuit secure processing unit ("SPU") that performs some secure processing outside of the SPU (see Ginter et al. patent disclosure FIG. 10 and associated text). Such a hybrid arrangement might be relatively more resistant to tampering than a software-only implementation. The assurance level III appliance 61C shown is a general purpose personal computer equipped with a hardware-based secure processing unit 132 providing and completely containing protected processing environment 108 (see Ginter et al. FIGS. 6 and 9 for example). A silicon-based special purpose integrated circuit security chip is relatively more tamper-resistant than implementations relying on software techniques for some or all of their tamper-resistance." ('721 __) - "Assurance level in this example may be assigned to a particular protected processing environment 108 at initialization (e.g., at the factory in the case of hardware-based secure processing units). Assigning assurance level at initialization time facilitates the use of key management (e.g., secure key exchange protocols) to enforce isolation based on assurance level. For example, since establishment of assurance level is done at initialization time, rather than in the field in this example, the key exchange

Claim Term	MS Construction

	mechanism can be used to provide new keys (assuming an assurance level has been established correctly)." ('721 __)
	
	- "The assurance level III appliance 61C shown is a general purpose personal computer equipped with a hardware-based secure processing unit 132 providing and completely containing protected processing environment 108 (see Ginter et al. FIGS. 6 and 9 for example). A silicon-based special purpose integrated circuit security chip is relatively more tamper-resistant than implementations relying on software techniques for some or all of their tamper-resistance."
	- "Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. Tamper resistant barriers may be used to protect this programming or other conditioning. The assurance levels described below are a measure or assessment of the effectiveness with which this programming or other conditioning is protected."
	- SN: 08/689,754: Amendment
	- Claims 9 and 30 cancelled.
	- Claims 1-2, 5-6, 10-15, 17-23, 26-27, 31-32, 34, 36, 38-43 amended. Some terms changed (e.g. work factor = security level); points in part to '107 spec'n (and in part to specific portions of '754 app.) to support definiteness of challenged claim terms; "execution spaces" "refers to a resource which can be used for execution of a program or process." (14));
	- "In accordance with this feature of the invention, verifying authority 100 supports all of these various categories of digital signatures, and system 50 uses key management to distribute the appropriate verification keys to different assurance level devices. For example, verifying authority 100 may digitally sign a particular load module 54 such that only hardware-only based server(s) 402(3) at assurance level XI may authenticate it. This compartmentalization prevents any load module executable on hardware-only servers 402(3) from executing on any other assurance level appliance (for example, software- only protected processing environment based support service 404(1))." (19:11)
	
	- "VDE, in its preferred embodiment, uses special purpose tamper resistant Secure Processing Units (SPUs) to help provide a high level of security for VDE processes and information storage and communication." ('193 4:3-7)
	
	- ('193 29:24-28); ('193 49:59-62); ('193 201:51-55); ('193 203:58-67); ('193 212:66-213:15)
	
	- "In order to allow, in the preferred embodiment, the ability to differentiate installations with different levels/degrees of trustedness/security, different certification key pairs may be used (e.g., different certification keys may be used to certify SPEs 503 then are used to certify HPEs 655)." (210:36)
	
	    "security level. To protect digital works against unauthorized uses, repositories need different degrees of physical security. Repositories handling extremely valuable works need greater security than ones for ordinary and portable use. The term security level refers to a sequence of levels ranging from low security to very high security."
	"Letting Loose the Light: Igniting Commerce in Electronic Publication," Stefik, draft 1994, 1995 (MSI028761)
	    "Security level: Different degrees of physical security – ranging from low security to very high security – for protecting digital works against unauthorized use. Repositories for handling extremely valuable works need greater security than those for ordinary and portable use."
	"Letting Loose the Light: Igniting Commerce in Electronic Publication," Stefik, in Internet Dreams, MIT 1996 (MSI028785)
	
	Prosecution History of '721 Patent:
	"please amend the application identified above as follows:
	IN THE CLAIMS
	Please cancel claims ... and amend claims 1, ... as follows:
	1. [Amended] A security method comprising:
	- (a) digitally signing a first load module with a first digital signature designating the first load

Claim Term	MS Construction
	module for use by a first device class; - (b) digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and[/or] security level [work factor substantially] different from the at least one of tamper resistance and/[or] security level [work factor] of the first device class; - (c) distributing the first load module for use by at least one device in the first device class; and - (d) distributing the second load module for use by at least one device in the second device class.'"" (pg. 1-2) "36. [Amended] A protected processing environment comprising: a first tamper resistant barrier having a first security level [work factor], a first secure execution space, and at least one arrangement within the first tamper resistant barrier that prevents the first secure execution space from executing the same executable accessed by a second [further] secure execution space having a second [further] tamper resistant barrier with a second [further] security level [work factor substantially] different from the first security level [work factor]." (pg. 10) "In the pending Office Action, the Examiner rejected claims 1-43 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. By this Amendment, Applicants have canceled claims ... and amended other claims to more appropriately define the present invention. ... In response to the Examiner's rejection, Applicants also have amended Claims 1-2, ... 36, ... to address issues raised by the Examiner." (pg. 13) 08/689,754 ('721), Amendment, 04/14/99, 1-2, 10, 13 Extrinsic: Security: The quality or state of being cost-effectively protected from undue losses (e.g. loss of goodwill, monetary loss, loss of ability to continue operations, etc.) (Longley) Level: 1. The degree of subordination of an item in a hierarchic arrangement. 3. The version of a program. (IBM) Level: 1. In computer security, see security level and integrity level. (Longley) Security level: In computer security, the combination of hierarchical classification and a set of non-hierarchical categories that represent the sensitivity of information. (Longley) Integrity level: In access control, a level of trustworthiness associated with a subject or object. (Longley) Security: The combination of integrity and secrecy, applied to data. (ITG, 5/12/95, IT00028295) Secrecy: The inability to obtain any information from data. (ITG, 5/12/95, IT00028294)
tamper resistance 721.1, 721.34, 900.155	Intrinsic: "The level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, and may vary widely." ('193 49:59-62) Extrinsic: Tamper-resistant Module: In data security, a device in which sensitive information, such as a master cryptographic key, is stored and cryptographic functions are performed. The device has one or more sensors to detect physical attacks, by an adversary trying to gain access to the stored information in which case the stored sensitive data is immediately destroyed. (Longley) Information Security Dictionary of Concepts, Standards, and Terms (1992) ("Tamper-resistant Module: In data security, a device in which sensitive information, such as a master cryptographic key, is stored and cryptographic functions are performed. The device has one or more sensors to detect physical

Claim Term	MS Construction
	attacks, by an adversary trying to gain access to the stored information in which case the stored sensitive data is immediately destroyed.") IT41530-49, IT51147-60 Neumann, Computer Related Risks (1995) at 349
Tamper resistant barrier 721.34	Intrinsic: "In addition, Applicants would like to draw the Examiner's attention to other sections of the specification in support of words or phrases cited by the Examiner as "indefinite." ... In claims ... 36 ... the term "barrier" is used as part of the phrase "tamper resistant barrier." This phrase is described in the specification on at least pages 7-8 and 46. In addition, the incorporated Ginter application describes tamper resistant barriers in a number of locations such as, for example, page 201." (pg. 13-14) (pages 7 and 46 of the original specification are '721 2:62-3:13 and 16:35-54 of the issued patent; page 201 of Ginter application SN 08/388,107 is '193 80:40-81:1) 08/689,754 ('721), Amendment, 04/14/99, p. 14 - SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions." ('193 59:48-53) - "Although block 1262 includes encrypted summary services information on the back up, it preferably does not include SPU device private keys, shared keys, SPU code and other internal security information to prevent this information from ever becoming available to users even in encrypted form." ('193 166:59-64) - "Briefly, the preferred example software-based PPE 650 installation process provides the following security techniques: encrypted software distribution, installation customized on a unique instance and/or electronic appliance basis, encrypted on-disk form, installation tied to payment method, unique software and data layout, and identifiable copies." (236:32) - " (c) if the load module has an associate digital signature , authenticating the digital signature at least one public key secured behind a tamper resistant barrier and therefore hidden from the user." ('721.9) - "A further attack technique might involve duplicating one installed operational material 3472 instance by coping the programs and data from one personal computer 3372B to another personal computer 3372C or emulator (see FIG. 67B, block 3364, and the "copy" arrow 3364A in FIG. 67A). The duplicated PPE instance could be used in a variety of ways, such as, for example, to place an imposter PPE 650 instance on-line and/or to permit further dynamic analysis." ('900 233:8-15) - "Various software protection techniques detailed above in connection with FIG. 10 may provide software-based tamper resistant barrier 674 within a software-only and/or hybrid software/hardware protected processing environment 650. The following is an elaboration on those above-described techniques. These software protection techniques may provide, for example, the following: An on-line registration process that results in the creation of a shared secret between the registry and the PPE 650 instance—used by the registry to create content and transactions that are meaningful only to specific PPE instance. An installation program (that may be distinct from the PPE operational material software) that creates a customized installation of the PPE software unique to each PPE instance and/or associate electronic appliance 600. Camouflage protections that make it difficult to reverse engineer the PPE 650 operational materials during PPE 650 operation. Integrity checks performed during PPE 650 operation (e.g., during on-line interactions with trusted servers) to detect compromise. In general, the software-based tamper resistant barrier 674 may establish "trust" primarily through uniqueness and complexity." ('900 235:30-57)- - ('900 243:3-9); ('193 80:40-65, Fig. 10); ('900 230:61-65); ('900 233:24-33); ('900 235:30-56); ('900 236:9-15)

Claim Term	MS Construction
	Extrinsic: Tamper-resistant Module: In data security, a device in which sensitive information, such as a master cryptographic key, is stored and cryptographic functions are performed. The device has one or more sensors to detect physical attacks, by an adversary trying to gain access to the stored information in which case the stored sensitive data is immediately destroyed. (Longley) "The "tamper-resistant module" is physically strong and destroys secrets when opened, and the software running inside has been checked for integrity;" (Davies) "The host computer is provided with a specially, physically secure module containing all the secret information which must be protected. In the IBM papers it is called the 'Cryptographic Facility': we shall call it a 'Tamper Resistant Module' (TRM)." (Davies)
tamper resistant software 900.155	Intrinsic: "Operational materials 3472 may then decrypt the next program segment dynamically ... This mechanism increases the tamper-resistance of the executable code--thus providing additional tamper resistance for PPE operations." ('900 243:3-8) Extrinsic: Tamper-resistant Module: In data security, a device in which sensitive information, such as a master cryptographic key, is stored and cryptographic functions are performed. The device has one or more sensors to detect physical attacks, by an adversary trying to gain access to the stored information in which case the stored sensitive data is immediately destroyed. (Longley) "Tamper resistant software resists observation and modification." Aucsmith, D., Tamper Resistant Software, 1ˢᵗ Workshop on Information Hiding, May 30, 1996.
use 912.8, 912.35, 861.58, 193.19, 891.1, 683.2, 721.1	Intrinsic: - Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving. - Content (executables for example) delivered with proof of delivery and/or execution or other use. - "In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:24-30) - "Some or all of the back up files may be packaged within an administrative object and transmitted for analysis, transportation, or other uses." ('193 167:45-48) - 4. "to securely control access and other use, including distribution of records, documents, and notes associated with the case." ('193 274:34-36) - "Thus wrapped, a VDE object may be distributed to the recipient without fear of unauthorized access and/or other use. The one or more authorized users who have received an object are the only parties who may open that object and view and/or manipulate and/or otherwise modify its contents and VDE secure auditing ensures a record of all such user content activities." ('193 277:15-21) - "These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc." ('193 9:24-27) - "VDE provides a secure, distributed electronic transaction management system for controlling the distribution and/or other usage of electronically provided and/or stored information." ('193 9:36-39) - "As a result, VDE supports most types of electronic information and/or appliance: usage control (including distribution), security, usage auditing, reporting, other administration, and payment arrangements." ('193 13:50-53) - Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving.

Claim Term	MS Construction
	- Content (executables for example) delivered with proof of delivery and/or execution or other use. - "In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:24-31) - "Some or all of the back up files may be packaged within an administrative object and transmitted for analysis, transportation, or other uses." ('193 6:24-) - "Thus wrapped, a VDE object may be distributed to the recipient without fear of unauthorized access and/or other use. The one or more authorized users who have received an object are the only parties who may open that object and view and/or manipulate and/or otherwise modify its contents and VDE secure auditing ensures a record of all such user content activities." ('193 277:15-21) - "These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc". ('193 9:24-27) - "VDE provides a secure, distributed electronic transaction management system for controlling the distribution and/or other usage of electronically provided and/or stored information." ('193 9:36-39) - "As a result, VDE supports most types of electronic information and/or appliance: usage control (including distribution), security, usage auditing, reporting, other administration, and payment arrangements." ('193 13:50-53) - "SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected. ('193 59:48-59) - "Once the information is downloaded, the now-initialized PPE 650 can discard (or simply not use) the manufacturing key." ('193 212:57-59) Extrinsic: User: A person using a InterTrust node to perform some function (i.e., acting in some role). A user is identified with respect to the node by a user ID: (ITG, 5/12/95, IT00028300) User ID: Locally to a InterTrust node, each InterTrust user has an ID associated with a user name and authentication (e.g., password). In some deployments, there may be only one user, and access to the machine may be considered sufficient authentication; in such cases, the user ID concept may not be visible to the user even though it is present in the implementation. (ITG, 5/12/95, IT00028301) Use: To use an object is to access the content. This involves the processes of controlling and metering the use of the property and creating audit trail records on the use. (VDE ROI DEVICE v1.0a 9 Feb 1994, IT00008570)
user controls 683.2	Intrinsic: - "PPE 650 may perform various tests on the inputted item and/or other results of the user interaction provided by block 4512E in accordance with one or more user controls." ('683 39:19-21) ('193 26:39-67) "support user interaction through: ... (c) VDE aware applications which, as a result of the use of a VDE API and/or a transaction management (for example, ROS based) programming language embeds VDE "awareness" into commercial or internal software (application programs, games, etc.) so that VDE user control information and services are seamlessly integrated into such software .... For example, in a VDE aware word processor application, a user may be able to "print" a document into a VDE content container object, applying specific control information by selecting from amongst a series of different

Claim Term	MS Construction
	menu templates for different purposes (for example, a confidential memo template for internal organization purposes may restrict the ability to "keep," that is to make an electronic copy of the memo)." ('193 26:39) Extrinsic: Control: A business rule that governs the use of content. (ITG, 1997-1998, ML00012B) Control: A set of rules and consequences that apply to a governed element. The term control can apply to either a control program or a control set. (ITG, 1997-2000, ML00012D) Control: *Control Element:* A data structure that giverns (*sic*) the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). *Control mechanism:* One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. * *Control object:* A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. *Control Parameter:* A data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself. (ITG, 3/7/1995, IT00709618, see footnote 2) Control: Defines rules and consequences for operations on a Property Chunk. A Control may be implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node.(ITG, 5/12/95, IT00028293) Control: A set of rules and consequences for operations on content, such as pricing, payment models, usage reporting etc. (ITG, 8/21/95, IT00032373, TD00068B) User: A person using a InterTrust node to perform some function (i.e., acting in some role). A user is identified with respect to the node by a user ID. (ITG, 5/12/95, IT00028300) User ID: Locally to a InterTrust node, each InterTrust user has an ID associated with a user name and authentication (e.g., password). In some deployments, there may be only one user, and access to the machine may be considered sufficient authentication; in such cases, the user ID concept may not be visible to the user even though it is present in the implementation. (ITG, 5/12/95, IT00028301) Extrinsic: User: 1. A person who requires the services of a computing system. 2. Any person or any thing that may issue or receive commands and messages to or from the information processing system. (IBM) User: 1. In communications security, any person who interacts directly with a network system. 4. In computer security, people who can access an AIS either by direct connections or indirect connections. (Longley) Control: The determination of the time and order in which the parts of a data processing system and the devices that contain those parts perform the input, processing, storage, and output functions.(IBM)
validity 912.8	Intrinsic: - "One of the functions SPU 500 may perform is to validate/authenticate VDE objects 300 and other items. Validation/authentication often involves comparing long data strings to determine whether they compare in a predetermined way." ('193 67:56-60) - ('193 73:24-25); ('193 73:26); ('193 78:6-17); ('193 87:47-55); ('193 112:46-61); ('193 210:28-35) Extrinsic: Validation: 1. In Cryptography, the process of checking the data integrity of a message, or selected parts of a message. (Longley) Validity Check: The process of analyzing data to determine whether it conforms to predetermined

Claim Term	MS Construction
	completeness and consistency parameters. (Microsoft Computer Dictionary, 3rd ed. 1997) "Validate – resolve references to other objects, check 'parameters'" (IT00051955)
Virtual distribution environment 900.155	Intrinsic: '193 203:58-67; '193 2:22 through conclusion of Background and Summary "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See 900.155 for Prosecution History limitations. "With respect to the remaining issues, Applicants respectfully disagree. For example, the Examiner objects to the use of "environment" as indefinite and unclear. This word, however, is not used in isolation, but rather in the context of several longer phrases, all of which are defined in the specification. The phrase "protected processing environment," for example, is used in Claims 11 and 15-18 and described on at least, for example, pages 7-8 and 25 of the specification. The term "virtual distribution environment" used in Claim 11 is described, for example, on page 7 of the specification. The terms are also described in the commonly copending application Serial Number 08/388,107 of Ginter et al., filed 13 February 1995, entitled "System and Methods for Secure Transaction Management and Electronic Rights Protection." A copy of the incorporated Ginter application can be provided to the Examiner upon request." (pg. 13-14) (pages 7, 7-8 and 25 of the original specification are '721 2:62-3:13, 2:62-3:34 and 8:6-28 of the issued patent) 08/689,754 ('721), Amendment, 04/14/99, p. 13 - VDE supports a model wide, distributed security implementation which creates a single secure "virtual" transaction processing and information storage environment. VDE enables distributed VDE installations to securely store and communicate information and remotely control the execution processes and the character of use of electronic information at other VDE installations and in a wide variety of ways; ('193 21:57-65) - The rights protection problems solved by the present invention are electronic versions of basic societal issues. These issues include protecting property rights, protecting privacy rights, properly compensating people and organizations for their work and risk, protecting money and credit, and generally protecting the security of information. ('193 4:8-13) - The present invention provides a new kind of "virtual distribution environment" (called "VDE" in this document) that secures, administers, and audits electronic information use. ('193 2:24-27) - A fundamental problem for electronic content providers is extending their ability to control the use of proprietary information. Content providers often need to limit use to authorized activities and amounts. Participants in a business model involving, for example, provision of movies and advertising on optical discs may include actors, directors, script and other writers, musicians, studios, publishers, distributors, retailers, advertisers, credit card services, and content end-users. These participants need the ability to embody their range of agreements and requirements, including use limitations, into an "extended" agreement comprising an overall electronic business model. This extended agreement is represented by electronic content control information that can automatically enforce agreed upon rights and obligations. Under VDE, such an extended agreement may comprise an electronic contract involving all business model participants. Such an agreement may alternatively, or in addition, be made up of electronic agreements between subsets of the business model participants. Through the use of VDE, electronic commerce can function in the same way as traditional commerce-that is commercial relationships regarding products and services can be shaped through the negotiation of one or more agreements between a variety of parties. ('193 2:37-60) - "Protecting the rights of electronic community members involves a broad range of technologies. VDE combines these technologies in a way that creates a "distributed" electronic rights protection

Claim Term	MS Construction
	"environment." This environment secures and protects transactions and other processes important for rights protection. VDE, for example, provides the ability to prevent, or impede, interference with and/or observation of, important rights related transactions and processes." ('193 3:63-4:3)
	- "VDE is a cost-effective and efficient rights protection solution that provides a unified, consistent system for securing and managing transaction processing. VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users." ('193 4:48-55)
	- In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed. ('193 6:24-30)
	- "A variety of capabilities are required to implement an electronic commerce environment. VDE is the first system that provides many of these capabilities and therefore solves fundamental problems related to electronic dissemination of information." ('193 8:16-20)
	- VDE offers an architecture that avoids reflecting specific distribution biases, administrative and control perspectives, and content types. Instead, VDE provides a broad-spectrum, fundamentally configurable and portable, electronic transaction control, distributing, usage, auditing, reporting, and payment operating environment. VDE is not limited to being an application or application specific toolset that covers only a limited subset of electronic interaction activities and participants. Rather, VDE supports systems by which such applications can be created, modified, and/or reused. As a result, the present invention answers pressing, unsolved needs by offering a system that supports a standardized control environment which facilitates interoperability of electronic appliances, interoperability of content containers, and efficient creation of electronic commerce applications and models through the use of a programmable, secure electronic transactions management foundation and reusable and extensible executable components. VDE can support a single electronic "world" within which most forms of electronic transaction activities can be managed. ('193 8:53-9:5)
	- "VDE can securely manage the integration of control information provided by two or more parties. As a result, VDE can construct an electronic agreement between VDE participants that represent a "negotiation" between, the control requirements of, two or more parties and enacts terms and conditions of a resulting agreement. VDE ensures the rights of each party to an electronic agreement regarding a wide range of electronic activities related to electronic information and/or appliance usage." ('193 9:52-61)
	- ""Hardware" 506 also contains long-term and short-term memories to store information securely so it can't be tampered with." ('193 60:1-3)
	- VDE prevents many forms of unauthorized use of electronic information, by controlling and auditing (and other administration of use) electronically stored and/or disseminated information. ('193 11:60-63)
	- Together, these VDE components comprise a secure, virtual, distributed content and/or appliance control, auditing (and other administration), reporting, and payment environment. ('193 13:14-17)
	- VDE can securely deliver information from one party to another concerning the use of commercially distributed electronic content. Even if parties are separated by several "steps" in a chain (pathway) of handling for such content usage information, such information is protected by VDE through encryption and/or other secure processing. Because of that protection, the accuracy of such information is guaranteed by VDE, and the information can be trusted by all parties to whom it is delivered. ('193 14:31-39)
	- VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a "virtual black box," a collection of distributed, very

Claim Term	MS Construction
	secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means. ('193 15:14-27) - VDE provides organization, community, and/or universe wide secure environments whose integrity is assured by processes securely controlled in VDE participant user installations (nodes). ('193 20:48-51) - - "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... "employ "templates" to ease the process of configuring capabilities of the present invention as they relate to specific industries or businesses. ...Given the very large range of capabilities and configurations supported by the present invention, reducing the range of configuration opportunities to a manageable subset particularly appropriate for a given business model allows the full configurable power of the present invention to be easily employed by "typical" users who would be otherwise burdened with complex programming and/or configuration design responsibilities template applications can also help ensure that VDE related processes are secure and optimally bug free by reducing the risks associated with the contribution of independently developed load modules, including unpredictable aspects of code interaction between independent modules and applications, as well as security risks associated with possible presence of viruses in such modules. ... As the context surrounding these templates changes or evolves, template applications provided under the present invention may be modified to meet these changes for broad use, or for more focused activities. ... Of course, templates may, under certain circumstances have fixed control information and not provide for user selections or parameter data entry." ('193 21:43-53 27:1-28:18) - "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... provide mechanisms to persistently maintain trusted content usage and reporting control information through both a sufficiently secure chain of handling of content and content control information and through various forms of usage of such content wherein said persistence of control may survive such use. Persistence of control includes the ability to extract information from a VDE container object by creating a new container whose contents are at least in part secured and that contains both the extracted content and at least a portion of the control information which control information of the original container and/or are at least in part produced by control information of the original container for this purpose and/or VDE installation control information stipulates should persist and/or control usage of content in the newly formed container. Such control information can continue to manage usage of container content if the container is "embedded" into another VDE managed object, such as an object which contains plural embedded VDE containers, each of which contains content derived (extracted) from a different source." ('193 21:43-53 28:45-65) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... Interoperability is fundamental to efficient electronic commerce. The design of the VDE foundation, VDE load modules, and VDE containers, are important features that enable the VDE node operating environment to be compatible with a very broad range of electronic appliances. ('193 21:43-45 34:25-30) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... securely support electronic currency and credit usage control, storage, and communication at, and between, VDE installations. ('193 21:43-45 36:49-51) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... requiring reporting and payment compliance by employing exhaustion of budgets and time ageing of keys. ('193 21:43-45 40:8-9) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... Because of the VDE security, including use of effective encryption, authentication, digital signaturing,

Claim Term	MS Construction
	and secure database structures, the records contained within a VDE card arrangement may be accepted as valid transaction records for government and/or corporate recordkeeping requirements. ('193 21:43-45 41:37-42) - Since all secure communications are at least in part encrypted and the processing inside the secure subsystem is concealed from outside observation and interference, the present invention ensures that content control information can be enforced. ('193 46:4-8) - An important feature of VDE is that it can be used to assure the administration of, and adequacy of security and rights protection for, electronic agreements implemented through the use of the present invention. ('193 46:51-54) - These are merely a few simple examples demonstrating the importance of ROS 602 ensuring that certain component assemblies 690 are formed in a secure manner. ROS 602 provides a wide range of protections against a wide range of "threats" to the secure handling and execution of component assemblies 690. ('193 85:15-20) - VDE further enables this process by providing a secure execution space in which the negotiation process(es) are assured of integrity and confidentiality in their operation. ('193 245:20-22) - "Taken together, and employed at times with VDE administrative objects and VDE security arrangements and processes, the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment." ('193 261:10-15) - For example, VDE 100 positively controls content access and usage, provides guarantee of payment for content used, and enforces budget limits for accessed content. ('193 240:53-56) - Such metering is a flexible basis for ensuring payment for content royalties, licensing, purchasing, and/or advertising. ('193 33:56-58) - The overall integrity and security of VDE 100 could ensure, in a coherent and centralized manner, that electronic reporting of tax related information (derived from one or more electronic commerce activities) would be valid and comprehensive. ('193 237:47-51) - Distributors 106 and financial clearinghouses 116 may themselves be audited based on secure records of their administrative activities and a chain of reliable, "trusted" processes ensures the integrity of the overall digital distribution process. This allows content owners, for example, to verify that they are receiving appropriate compensation based on actual content usage or other agreed-upon bases. ('193 254:66-255:5) - Because the control information is carried with each copy of a VDE protected document, and can ensure that central registries are updated and/or that originators are notified of document use, tracking can be prompt and accurate. ('193 281:14-16) - A final desirable feature of agreements in general (and electronic representations of agreements in particular) is that they be accurately recorded in a non-repudiatable form. In traditional terms, this involves creating a paper document (a contract) that describes the rights, restrictions, and obligations of all parties involved. This document is read and then signed by all parties as being an accurate representation of the agreement. Electronic agreements, by their nature, may not be initially rendered in paper. VDE enables such agreements to be accurately electronically described and then electronically signed to prevent repudiation. ('193 245:25-35) - As discussed above, a wide variety of techniques are currently being used to provide secure, trusted confidential delivery of documents and other items. Unfortunately, none of these previously existing mechanisms provide truly trusted, virtually instantaneous delivery on a cost-effective, convenient basis and none provide rights management and auditing through persistent, secure, digital information protection. In contrast, the present inventions provide the trustedness, confidentiality and security of a personal trusted courier on a virtually instantaneous and highly cost-effective basis. They provide techniques, systems and methods that can being to any form of electronic communications (including, but not

Claim Term	MS Construction
	limited to Internet and internal company electronic mail) an extremely high degree of trustedness, confidence and security approaching or exceeding that provided by a trusted personal courier. They also provide a wide variety of benefits that flow from rights management and secure chain of handling and control. ('683 5:20) - The Virtual Distribution Environment provides comprehensive overall systems, and wide arrays of methods, techniques, structures and arrangements, that enable secure, efficient electronic commerce and rights management on the Internet and other information superhighways and on internal corporate networks such as "Intranets". ('683 5:41) - "parties using the Virtual Distribution Environment can participate in commerce and other transactions in accordance with a persistent set of rules they electronically define." ('683 6:11) - "All of these various coordination steps can be performed nearly simultaneously, efficiently, rapidly and with an extremely high degree of trustedness based on the user of electronic containers 302 and the secure communications, authentication, notarization and archiving techniques provided in accordance with the present inventions." ('683 55:54) - "People are increasingly using secure digital containers to safely and securely store and transport digital content. One secure digital container model is the "DigiBox.TM." container developed by InterTrust Technologies, Inc. of Sunnyvale, Calif. The Ginter et al. patent specification referenced above describes many characteristics of this DigiBox.TM. container model—a powerful, flexible, general construct that enables protected, efficient and interoperable electronic description and regulation of electronic commerce relationship of all kinds, including the secure transport, storage and rights management interface with objects and digital information within such containers." ('861 1:35) - "Briefly, DigiBox containers are tamper-resistant digital containers that can be used to package any kind of digital information such as, for example, text, graphics, executable software, audio and/or video. The rights management environment in which DigiBox.TM. containers are used allows commerce participants to associate rules with the digital information (content). The rights management environment also allows rules (herein including rules and parameter data controls) to be securely associated with other rights management information, such as for example, rules, audit records created during use of digital information and administrative information associated with keeping the environment working properly, including ensuring rights and any agreements among parties. The DigiBox.TM.. electronic container can be used to store, transport and provide a rights management interfaces to digital information, related rules and other rights management information, as well as to other objects and/or data within a distributed, rights management environment. This arrangement can be used to provide electronically enforced chain of handling and control wherein rights management persists as a container moves from one entity to another. This capability helps support a digital rights management architecture that allows content rightsholders (including any parties who have system authorized interests related to such content, such as content republishes or even governmental authorities) to securely control and manage content, events, transactions, rules and usage consequences, including any required payment and/or usage reporting. This secure control and management continues persistently, protecting rights as content is delivered to, used by, and passed among creators, distributors, repurposes, consumers, payment disaggregators, and other value chain participants... " ('861 1:47) - "Use of a secure electronic container containers to transport items providers an unprecedented degree of security, trustedness and flexibility." ('683 8:50) - "Virtual distribution environment 100 is "virtual" because it does not require many of the physical "things" that used to be necessary to protect rights, ensure reliable and predictable distribution, and ensure proper compensation to content creators and distributors." ('193 53:23-27) - VDE allows the needs of electronic commerce participants, to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present all physical locations where VDE related contents is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing

Claim Term	MS Construction
	functions (including metering) that operate within a "virtual black box"" a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means. ('193 15:14-27)

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention ...VDE employs special purpose hardware distributed throughout some or all locations of a VDE implementation: a) said hardware controlling important elements of: content preparation (such as causing such content to be placed in a VDE content container and associating content control information with said content), content and/or electronic appliance usage auditing, content usage analysis, as well as content usage control; and b) said hardware having been designed to securely handle processing load module control activities, wherein said control processing activities may involve a sequence of required control factors" ('193 21:43-45 22:20-31)

- Physical facility and user identity authentication security procedures may be used instead of hardware SPUs at certain nodes, such as at an established financial clearinghouse, where such procedures may provide sufficient security for trusted interoperability with a VDE arrangement employing hardware SPUs at user nodes. ('193 45:60-65)

- An important part of VDE provided by the present invention is the core secure transaction control arrangement, herein called an SPU (or SPUs), that typically must be present in each user's computer, other electronic appliance, or network. SPUs provide a trusted environment for generating decryption keys, encrypting and decrypting information, managing the secure communication of keys and other information between electronic appliances (i.e. between VDE installations and/or between plural VDE instances within a single VDE installation), securely accumulating and managing audit trail, reporting, and budget information in secure and/or non-secure non-volatile memory, maintaining a secure database of control information management instructions, and providing a secure environment for performing certain other control and administrative functions. ('193 48:66-49:14)

- A hardware SPU (rather than a software emulation) within a VDE node is necessary if a highly trusted environment for performing certain VDE activities is required. ('193 49:15-17)

- ""Hardware" 506 also contains long-term and short-term memories to store information securely so it can't be tampered with." ('193 60:1-3)

- A VDE node's hardware SPU is a core component of a VDE secure subsystem and may employ some or all of an electronic appliance's primary control logic, such as a microcontroller, microcomputer or other CPU arrangement. This primary control logic may be otherwise employed for non VDE purposes such as the control of some or all of an electronic appliance's non-VDE functions. When operating in a hardware SPU mode, said primary control logic must be sufficiently secure so as to protect and conceal important VDE processes. For example, a hardware SPU may employ a host electronic appliance microcomputer operating in protected mode while performing VDE related activities, thus allowing portions of VDE processes to execute with a certain degree of security. ('193 49:33-46)

- As shown FIG. 6, in the preferred embodiment, an SPU 500 may be implemented as a single integrated circuit "chip" 505 to provide a secure processing environment in which confidential and/or commercially valuable information can be safely processed, encrypted and/or decrypted. ('193 63:48-52)

"SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 form being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected." ('193 59:48-59)

- "SPU 500 may be surrounded by a tamper-resistant hardware security barrier 502. Part of this security barrier 502 is formed by a plastic or other package in which an SPU "die" is encased. Because the processing occurring within, and information stored by, SPU 500 are not easily accessible to the |

Claim Term	MS Construction
	outside world, they are relatively secure from unauthorized access and tampering. All signals cross barrier 502 through a secure, controlled path provided by BIU 530 that restricts the outside world's access to the internal components within SPU 500. The secure, controlled path resists attempts form the outside world to access secret information and resources within SPU 500." ('193 63:60-64:5)

- Regulation is ensured by control information put in place by one or more parties. ('193 6:34-35)

-"Limited only by the VDE control information employed by content creators, other providers, and other pathway of handling and control participants, VDE allows a "natural" and unhindered flow of, and creation of, electronic content product models." ('193 297:25-29)

- As a result, the present invention answers pressing, unsolved needs by offering a system that supports a standardized control environment which facilitates interoperability of electronic appliances, interoperability of content containers, and efficient creation of electronic commerce applications and models through the use of a programmable, secure electronic transactions management foundation and reusable and extensible executable components. ('193 8:62-9:3)

- Independently, securely deliverable, component based control information allows efficient interaction among control information sets supplied by different parties. ('193 10:46-48)

- A significant facet of the present invention's ability to broadly support electronic commerce is its ability to securely manage independently delivered VDE component objects containing control information (normally in the form of VDE objects containing one or more methods, data, or load module VDE components). This independently delivered control information can be integrated with senior and other pre-existing content control information to securely form derived control information using the negotiation mechanisms of the present invention. All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used. This means that, for example, all load modules and any mediating data which are listed by the derived control information as required must be available and securely perform their required function. ('193 10:66-11:14)

- Content control information governs content usage according to criteria set by holders of rights to an object's contents and/or according to parties who otherwise have rights associated with distributing such content (such as governments, financial credit providers, and users). ('193 15:46-50)

- In part, security is enhanced by object methods employed by the present invention because the encryption schemes used to protect an object can efficiently be further used to protect the associated content control information (software control information and relevant data) from modification. ('193 15:51-55)

- Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... Content users, such as end-user customers using commercially distributed content (games, information resources, software programs, etc.), can define, if allowed by senior control information, budgets, and/or other control information, to manage their own internal use of content. ('193 21:43-45 29:3-8)

- Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... support the separation of fundamental transaction control processes through the use of event (triggered) based method control mechanisms. These event methods trigger one or more other VDE methods (which are available to a secure VDE sub-system) and are used to carry out VDE managed transaction related processing. These triggered methods include independently (separably) and securely processable component billing management methods, budgeting management methods, metering management methods, and related auditing management processes. As a result of this feature of the present invention, independent triggering of metering, auditing, billing, and budgeting methods, the present invention is able to efficiently, concurrently support multiple financial currencies (e.g. dollars, marks, yen) and content related budgets, and/or billing increments as well as very flexible content distribution models. ('193 21:43-45 42:21-38)

- support, complete, modular separation of the control structures related to (1) content event triggering, (2) auditing, (3) budgeting (including specifying no right of use or unlimited right of use), (4) billing, and (5) user identity (VDE installation, client name, department, network, and/or user, etc.). The

Claim Term	MS Construction
	independence of these VDE control structures provides a flexible system which allows plural relationships between two or more of these structures, for example, the ability to associate a financial budget with different event trigger structures (that are put in place to enable controlling content based on its logical portions). Without such separation between these basic VDE capabilities, it would be more difficult to efficiently maintain separate metering, budgeting, identification, and/or billing activities which involve the same, differing (including overlapping), or entirely different, portions of content for metering, billing, budgeting, and user identification, for example, paying fees associated with usage of content, performing home banking, managing advertising services, etc. VDE modular separation of these basic capabilities supports the programming of plural, "arbitrary" relationships between one or differing content portions (and/or portion units) and budgeting, auditing, and/or billing control information. ('193 42:39-63)

- The virtual distribution environment 100 prevents use of protected information except as permitted by the "rules and controls" (control information). For example, the "rules and controls" shown in FIG. 2 may grant specific individuals or classes of content users 112 "permission" to use certain content. They may specify what kinds of content usage are permitted, and what kinds are not. They may specify how content usage is to be paid for and how much it costs. As another example, "rules and controls" may require content usage information to be reported back to the distributor 106 and/or content creator 102. ('193 56:26-35)

- "ROS VDE functions 604 may be based on segmented, independently loadable executable "component assemblies" 690. These component assemblies 690 are independently securely deliverable. The component assemblies 690 provided by the preferred embodiment comprise code and data elements that are themselves independently deliverable.... These component assemblies 690 are the basic functional unit provided by ROS 602. The component assemblies 690 are executed to perform operating system or application tasks. Thus, some component assemblies 690 may be considered to be part of the ROS operating system 602, while other component assemblies may be considered to be "applications" that run under the support of the operating system." ('193 83:12-29)

- "As mentioned above, ROS 602 provides several layers of security to ensure the security of component assemblies 690. One important security layer involves ensuring that certain component assemblies 690 are formed, loaded and executed only in secure execution space such as provided within an SPU 500." ('193 87:33-38)

- "Methods 1000 perform the basic function of defining what users (including, where appropriate, distributions, client administration, etc.), can and cannot do with an object 300." ('193 128:30-33)

- "Container 152 in this example further includes an electronic control set 188 describing conditions under which the power may be exercised. Controls 188 define the power(s) granted to each of the participants – including (in this example) conditions or limitations for exercising these powers. Controls 188 may provide the same powers and/or conditions of use for each participant, or they may provide different powers and/or conditions of use for each participant." ('712 220: 1-8)

- "...content creators and rights owners can register permissions with the rights and permissions clearinghouses 400 in the form of electronic "control sets." These permissions can specify what consumers can and can't do with digital properties, under what conditions the permissions can be exercised and the consequences of exercising the permissions." ('712 72:2-7)

- "This "channel 0" "open channel" task may then issue a series of requests to secure database manager 566 to obtain the "blueprint" for constructing one or more component assemblies 690 to be associated with channel 594 (block 1127). In the preferred embodiment, this "blueprint" may comprise a PERC 808 and/or URT 464." ('193 112:46-51)

- In part, security is enhanced by object methods employed by the present invention because the encryption schemes used to protect an object can efficiently be further used to protect the associated content control information (software control information and relevant data) from modification. ('193 15:51-55)
- FIG. 5A shows how the virtual distribution environment 100, in a preferred embodiment, may package information elements (content) into a "container" 302 so the information can't be accessed |

Claim Term	MS Construction

except as provided by its "rules and controls." Normally, the container 302 is electronic rather than physical. Electronic container 302 in one example comprises "digital" information having a well defined structure. Container 302 and its contents can be called an "object 300." ('193 58:39-46)

- "Moreover, when any new VDE object 300 arrives at an electronic appliance 600, the electronic appliance must "register" the object within object registry 450 so that it can be accessed." ('193 153:56-59)

- "Even if the object is stored locally to the VDE node, it may be stored as a secure or protected object so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security requisites needed to access the object." ('193 192:14-19)
- "ACCESS method 2000 reads the ACCESS method MDE from the secure database, reads it in accordance with the ACCESS method DTD, and loads encrypted content source and routing information based on the MDE (blocks 2010, 2012). This source and routing information specifies the location of the encrypted content. ACCESS method 2000 then determines whether a connection to the content is available (decision block 2014). This "connection" could be, for example, an on-line connection to a remote site, a real-time information feed, or a path to a secure/protected resource, for example. If the connection to the content is not currently available ("No" exit of decision block 2014), then ACCESS method 2000 takes steps to open the connection (block 2016). If the connection fails (e.g., because the user is not authorized to access a protected secure resource), then the ACCESS method 2000 returns with a failure indication (termination point 2018)." ('193 192:36-52)

- "It also employs a software object architecture for VDE content containers that carries protected content and may also carry both freely available information (e.g., summary, table of contents) and secured content control information which ensures the performance of control information." ('193 15:41-46)

- "In this example, creator 102 may employ one or more application software programs and one or more VDE secure subsystems to place unencrypted content into VDE protected form (i.e., into one or more VDE content containers)." ('193 315:53-56)

- "The Ginter et al. patent specification referenced above describes many characteristics of this DigiBox™ container model, a powerful, flexible, general construct that enables protected, efficient and interoperable electronic description and regulation of electronic commerce relationships of all kinds..." ('861 1:39)]

- "The node and container model described above and in the Ginter et al. patent specification (along with similar other DigiBox/VDE (Virtual Distribution Environment) models) has nearly limitless flexibility." ('861 2:37)

- Therefore, the container creation and usage tools must themselves be secure in the sense that they must protect certain details about the container design. This additional security requirement can make it even more difficult to make containers easy to use and to provide interoperability. ('861 4:59)

- "FIG. 88 illustrates secure electronic container 302 as an attaché handcuffed to the secure delivery person's wrist. Once again, container is shown as a physical thing for purposes of illustrations only – in the example it is preferably electronic rather than physical, and comprises digital information having a well-defined structure (see FIG. 5A). Special mathematical techniques known as "cryptography" can be used to make electronic container 302 secure so that only intended recipient 4056 can open the container and access the electronic document (or other items) 4054 it contains." ('683 15:61)

- "Appliance 600B may deliver the digital copy of item 4054 within container 302 and/or protect the item with seals. Electronic fingerprints, watermarks and/.or other visible and/or hidden markings to provide a "virtual container or some of the security or other characteristics of a container (for example, the ability to associate electronic controls with the item). ('683 18:)

- "For example, defendant's attorney 5052 can specify one container 302 for opening by his co-counsel, client or client in-house counsel, and program another container 302 for opening only by opposing (plaintiff's) counsel 5050. Because of the unique trustedness features provided by system 4050, the defendant's attorney 5052 can have a high degree of trust and confidence that only the

Claim Term	MS Construction
	authorized parties will be able to open the respective containers and access the information they contain." ('683 56:17)

- "The "container" concept is a convenient metaphor used to give a name to the collection of elements *required to make use of content* or to perform an administrative-type activity." ('193 127:30-32)

- "the virtual distribution environment 100, in a preferred embodiment, may package information elements (content) into a "container" 302 so the information can't be accessed except as provided by its "rules and controls."" ('193 58:39-43)

- "VDE 100 provides a media independent container model for encapsulating content." ('193 127:2-3)

- "The electronic form of a document is stored as a VDE container (object) associated with the specific client and/or case. The VDE container mechanism supports a hierarchical ordering scheme for organizing files and other information with a container; this mechanism may be used to organize the electronic copies of the documents within a container, A VDE container is associated with specific access control information and rights that are described in one or more permissions control information sets (PERCs) associated with that container. In this example, only those members of the law firm who possess a VDE instance, an appropriate PERC, and the VDE object that contains the desired document, may use the document." ('193 274:52-64)

- "The situation is no better for processing documents within the context of ordinary computer and network systems. Although said systems can enforce access control information based on user identity, and can provide auditing mechanism for tracking accesses to files, these are low-level mechanisms that do not permit tracking or controlling the flow of content. In such systems, because document content can be freely copied and manipulated, it is not possible to determine where documents content has gone, or where it came from." ('193 281:27-35)

- "Secure containers 302 may be used to encapsulate the video and audio being exchanged between electronic kiosk appliances 600, 600' to maintain confidentiality and ensure a high degree of trustedness.

- "Because container 152 can only be opened within a secure protected processing environment 154 that is part of the virtual distribution environment described in the above-referenced Ginter et al. patent disclosure" - "The present invention provides a new kind of "virtual distribution environment" (called "VDE" in this document) that secures, administers, and audits electronic information use. VDE also features fundamentally important capabilities for ...." ('193 2:24-28)

- "the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment." ('193 261:12-15)

- "The inability of conventional products to be shaped to the needs of electronic information providers and users is sharply in contrast to the present invention. Despite the attention devoted by a cross-section of America's largest telecommunications, computer, entertainment and information provider companies to some of the problems addressed by the present invention, only the present invention provides commercially secure, effective solutions for configurable, general purpose electronic commerce transaction/distribution control systems." ('193 2:13-22)

- "The configurability provided by the present invention is particularly critical for supporting electronic commerce, that is enabling businesses to create relationships and evolve strategies that offer competitive value. Electronic commerce tools that are not inherently configurable and interoperable will ultimately fail to produce products (and services) that meet both basic requirements and evolving needs of most commerce applications." ('193 16:41-48)

- "VDE also extends usage control information to an arbitrary granular level (as opposed to a file based level provided by traditional operating systems) and ...." ('193 275:8-11)

- Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: ...." ('193 21:43-45)

- "A significant facet of the present invention's ability to broadly support electronic commerce is its

Claim Term	MS Construction
	ability to securely manage independently delivered VDE component objects containing control information ...." ('193 10:66-11:2)

-"Some of the key factors contributing to the configurability intrinsic to the present invention include: ...." ('193 16:66-67)

-"The scalable transaction management/auditing technology of the present invention will result in more efficient and reliable interoperability ...." ('193 34:9-11)

-"the present invention answers pressing, unsolved needs by offering a system that supports a standardized control environment which facilitates interoperability of electronic appliances, interoperability of content containers, and efficient creation of electronic commerce applications and models through the use of a programmable, secure electronic transactions management foundation and reusable and extensible executable components." ('193 8:63-9:3)

-"The design of the VDE foundation, VDE load modules, and VDE containers, are important features that enable the VDE node operating environment to be compatible with a very broad range of electronic appliances." ('193 34:26-30)

-"The ability to optionally incorporate different methods 1000 with each object is important to making VDE 100 highly configurable." ('193 128:28-30)

-"An important feature of VDE is that it can be used to assure the administration of, and adequacy of security and rights protection for, electronic agreements implemented through the use of the present invention." ('712 168:22-25)

-"In this example, both the address request 602 and the responsive information 604 are contained within secure electronic containers 152 in order to maintain the confidentiality and integrity of the requests and responses. In this way, for example, outside eavesdroppers cannot tell who sender 95(1) wants to communicate with or what information he or she needs to perform communications with or what information he or she needs to perform the communications – and the directory responses cannot be "spoofed" to direct the requested message to another location." ('712 12:15-22)

Components: "On the other hand, if the information to be exchanged has already been secured and/or is available without authentication (e.g., certain catalog information, containers that have already been encrypted and do not require special handling, etc.), the "weaker" for of login/password may be used." ('193 290:57-62)

Components: "VDE provides means to securely combine content provided at different times, by differing sources, and/or representing different content types. These types, timings, and/or different sources of content can be employed to form a complex array of content within a VDE content container objects, each containing different content whose usage can be controlled, at least in part, by its own container's set of VDE content control information." ('193 397:35-)

Container-Related Methods: "Although methods 1000 can have virtually unlimited variety and some may even be user-defined, certain basic "use" type methods are preferably used in the preferred embodiment to control most of the more fundamental object manipulation and other functions provided by VDE 100. For example, the following high level methods would typically be provided for object manipulation; OPEN method, READ method, WRITE method, CLOSE method. An OPEN method is used to control opening a container so its content may be accessed. A READ method is used to control access to contents in a container. A WRITE method is used to control the insertion of contents into a container. A CLOSE method is used to close a container that has been opened." ('193 183:12-29)[5]

- "DESTROY method 2180 removes the ability of a user to use an object by destroying the URT the user requires to access the object. In the preferred embodiment, ... DESTROY method 2180 may than call a WRITE and/or ACCESS method to write information which will corrupt (and thus destroy) the header and/or other important parts of the object (block 2186). DESTROY method 2180 may then mark one or more of the control structures (e.g., the URT) as damaged by writing appropriate information to control structure (blocks 2188, 2190)." ('193 198:41-45)

- "PANIC method 2200 may prevent the user from further accessing the object currently being accessed |

Claim Term	MS Construction

by, for example, destroying the channel being used to access the object and marking one or more of the control structures (e.g., the URT) associated with the user and object as damaged.(blocks 2206, and 2208-2210, respectively). Because the control structure is damaged, the VDE node will need to contact an administrator to obtain a valid control structure(s) before the user may access the same object again." ('193 198:60-199:2)

- "EXTRACT method 2080 is used to copy or remove content from an object and place it into a new object. In the preferred embodiment, the EXTRACT method 2080 does not involve any release of content, but rather simply takes content from one container and places it into another container, both of which may be secure. Extraction of content differs from release in that the content is never exposed outside a secure container." ('193 194:13-20)

- "Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility." ('683 8:50)

-"Electronic delivery person 4060 can deliver the electronic version of item 4054 within secure container attaché case 302 from personal computer 4116' to another personal computer 4116 operated by recipient 4056." ('683 20:27)

- "Because these transactions are conducted using VDE and VDE secure containers, those observing the communications learn no more than the fact that the parties are communicating." ('712 310:1-3)

- "VDE in one example provides a "virtual silicon container" ("virtual black box") in that several different instances of SPU 500 may securely communicate together to provide an overall secure hardware environment that "virtually" exists at multiple locations and multiple electronic appliances 600. FIG. 87 shows one model 3600 of a virtual silicon container. This virtual container model 3600 includes a content creator 102, a content distributor 106, one or more content redistributors 106a, one or more client administrators 700, one or more client users 3602, and one or more clearinghouses 116. Each of these various VDE participants has an electronic appliance 600 including a protected processing environment 655 that may comprise, at least in part, a silicon-based semiconductor hardware element secure processing unit 500. The various SOUs 500 each encapsulate a part of the virtual distribution environment, and thus, together form the virtual silicon container 3600." ('193 317:58-318:8)

-"uses tools to transform digital information(such as electronic books, databases, computer software and movies) into protected digital packages called "objects." Only those consumers (or other along the chain of possession such as redistributor) who receive permission from a distributor 106 can open these packages. VDE packaged content can be constrained by "rules and control information."" ('193 254:18-25)

-"To open VDE package and make use of its content, and end-user must have permission." ('193 254:45-46)

- "place unencrypted content into VDE protected form (i.e., into one or more VDE content containers)." ('193 315:55-56)

- "VDE can protect a collection of rights belonging to various parties having in rights in, or to, electronic information. This information may be at one location or dispersed across (and/or moving between) multiple locations. The information may pass through a "chain" of distributors and a "chain" of users. Usage information may also be reported through one or more "chains" of parties. In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:18-31)

- All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used. ('193 11:8-11)

- "VDE provides important mechanisms for both enforcing commercial agreements and enabling the protection of privacy rights. VDE can securely deliver information from one party to another

Claim Term	MS Construction
	concerning the use of commercially distributed electronic content. Even if parties are separated by several "steps" in a chain (pathway) of handling for such content usage information, such information is protected by VDE through encryption and/or other secure processing. Because of that protection, the accuracy of such information is guaranteed by VDE, and the information can be trusted by all parties to whom it is delivered." ('193 14:29-39) - VDE ensures that certain prerequisites necessary for a given transaction to occur are met. This includes the secure execution of any required load modules and the availability of any required, associated data. ('193 20:27-30) - Required methods (methods listed as required for property and/or appliance use) must be available as specified if VDE controlled content (such as intellectual property distributed within a VDE content container) is to be used. ('193 43:37-41) - "Since all secure communications are at least in part encrypted and the processing inside the secure subsystem is concealed from outside observation and interference, the present invention ensures that content control information can be enforced. ('193 46:4-8) - This control information can determine, for example: (1) How and/or to whom electronic content can be provided, for example, how an electronic property can be distributed; (2) How one or more objects and/or properties, or portions of an object or property, can be directly used, such as decrypted, displayed, printed, etc; .... ('193 46:17-24) ""Hardware" 506 also contains long-term and short-term memories to store information securely so it can't be tampered with." ('193 60:1-3) "A feature of VDE provided by the present invention is that certain one or more methods can be specified as required in order for a VDE installation and/or user to be able to use certain and/or all content. ('193 43:47-50) The virtual distribution environment 100 prevents use of protected information except as permitted by the "rules and controls" (control information). ('193 56:26-28) - As mentioned above, virtual distribution environment 100 "associates" content with corresponding "rules and controls," and prevents the content from being used or accessed unless a set of corresponding "rules and controls" is available. The distributor 106 doesn't need to deliver content to control the content's distribution. The preferred embodiment can securely protect content by protecting corresponding, usage enabling "rules and controls" against unauthorized distribution and use. ('193 57:18-26) - Since no one can use or access protected content without "permission" from corresponding "rules and controls," the distributor 106 can control use of content that has already been (or will in the future be) delivered. ('193 57:30-33) - SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. ('193 59:48-55) - Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, redistributing (including to what one or more parties), and/or saving. - In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed. ('193 6:24-30) - to securely control access and other use, including distribution of records, documents, and notes associated with the case, ('193 274:34-36)

Claim Term	MS Construction

- Thus wrapped, a VDE object may be distributed to the recipient without fear of unauthorized access and/or other use. ('193 277:16-17)

- These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc.('193 9:24-27)

- VDE provides a secure, distributed electronic transaction management system for controlling the distribution and/or other usage of electronically provided and/or stored information. ('193 9:36-39)

- "The doctor 5000 may then send container 301(1) to a trusted go-between 4700. ...For example, the trusted go-between 4700 in one example has no access to the content of the container 302(1), but does have a record of a seal of the contents." ('683 53:40)

- "FIG. 116 shows example steps that may be performed by PPE 650 in response to an "open" or "view" event. In this example, PPE 650 may - - upon allowing recipient 4056 to actually interact with the item 4054--...PPE 650 may then release the image 40681 and/or the data 4068D to the application running on electronic appliance 600—electronic fingerprinting or watermarking the released content if appropriate (FIG. 116, block 4625C). ('683 42:38)

- FIG. 5A shows how the virtual distribution environment 100, in a preferred embodiment, may package information elements (content) into a "container" 302 so the information can't be accessed except as provided by its "rules and controls." ('193 58:39-43)

- Each VDE participant in a VDE pathway of content control information may set methods for some or all of the content in a VDE container, so long as such control information does not conflict with senior control information already in place with respect to:
(1) certain or all VDE managed content,
(2) certain one or more VDE users and/or groupings of users,
(3) certain one or more VDE nodes and/or groupings of nodes, and/or
(4) certain one or more VDE applications and/or arrangements. ('193 44:6-17)

- "All participants of VDE 100 have the innate ability to participate in any role." ('193 256:50-51)
- "Any VDE user 112 may assign the right to process information or perform services on their behalf to the extend allowed by senior control information." ('193 257:17-20)

- "PERC and URT structures provide a mechanism that may be used to provide precise electronic representation of rights and the controls associated with those rights. VDE thus provides a "vocabulary" and mechanism by which users and creators may specify their desires." ('193 245:11-)

- "VDE provides comprehensive and configurable transaction management, metering and monitoring technology." ('193 3:34)

- VDE may be combined with, or integrated into, many separate computers and/or other electronic appliances. These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc. The secure subsystem in the preferred embodiment comprises one or more "protected processing environments", one or more secure databases, and secure "component assemblies" and other items and processes that need to be kept secured. VDE can, for example, securely control electronic currency, payments, and/or credit management (including electronic credit and/or currency receipt, disbursement, encumbering, and/or allocation) using such a "secure subsystem." ('193 9:22)

- "In addition VDE:
(a) is very configurable, modifiable, and re-usable;
(b) supports a wide range of useful capabilities that may be combined in different ways to accommodate most potential applications;
(c) operates on a wide variety of electronic appliances ranging from hand-held inexpensive devices to large mainframe computers;

Claim Term	MS Construction
	(d) is able to ensure the various rights of a number of different parties, and a number of different rights protection schemes, simultaneously; (e) is able to preserve the rights of parties through a series of transactions that may occur at different times and different locations; (f) is able to flexibly accommodate different ways of securely delivering information and reporting usage; and (g) provides for electronic analogues to "real" money and credit, including anonymous electronic cash, to pay for products and services and to support personal (including home) banking and other financial activities." ('193 4:57) - It can provide efficient, reusable, modifiable, and consistent means for secure electronic content distribution, usage control, usage payment, usage auditing, and usage reporting. ('193 8:26) - VDE offers an architecture that avoids reflecting specific distribution biases, administrative and control perspectives, and content types. Instead, VDE provides a broad-spectrum, fundamentally configurable and portable, electronic transaction control, distributing, usage, auditing, reporting, and payment operating environment. ('193 8:53) - The present invention allows content providers and users to formulate their transaction environment to accommodate: (1) desired content models, content control models, and content usage information pathways, (2) a complete range of electronic media and distribution means, (3) a broad range of pricing, payment, and auditing strategies, (4) very flexible privacy and/or reporting models, (5) practical and effective security architectures, and (6) other administrative procedures that together with steps (1) through (5) can enable most "real world" electronic commerce and data security models, including models unique to the electronic world. ('193 10:11) - Because of the breadth of issues resolved by the present invention, it can provide the emerging "electronic highway" with a single transaction/distribution control system that can, for a very broad range of commercial and data security models, ensure against unauthorized use of confidential and/or proprietary information and commercial electronic transactions. ('193 17:22) - "A feature of the present invention provides for payment means supporting flexible electronic currency and credit mechanisms, including the ability to securely maintain audit trails reflecting information related to use of such currency or credit.' ('193 33:58) - "the end-to-end nature of VDE applications, in which content 108 flows in one direction, generating reports and bills 118 in the other, makes it possible to perform "back-end" consistency checks." ('193 223:17) - By way of non-exhaustive summary, these present inventions provide a highly secure and trusted item delivery and agreement execution services providing the following features and functions: Trustedness and security approaching or exceeding that of a personal trusted courier. Instant or nearly instant delivery. Optional delayed delivery ("store and forward"). Broadcasting to multiple parties. Highly cost effective. Trusted validation of item contents and delivery. Value Added Delivery and other features selectable by the sender and/or recipient. Provides electronic transmission trusted auditing and validating. Allows people to communicate quickly, securely, and confidentially. Communications can later be proved through reliable evidence of the communications transaction— providing non-repudiatable, certain, admissible proof that a particular communications transaction occurred. Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving.

Claim Term	MS Construction
	Supports persistent rights and rules based document workflow management at recipient sites. System may operate on the Internet, on internal organization and/or corporate networks ("intranets" irrespective of whether they use or offer Internet services internally), private data networks and/or using any other form of electronic communications. System may operate in non-networked and/or intermittently networked environments. Legal contract execution can be performed in real time, with or without face to face or ear-to-ear personal interactions (such as audiovisual teleconferencing, automated electronic negotiations, or any combination of such interactions) for any number of distributed individuals and/or organizations using any mixture of interactions. The items delivered and/or processed may be any "object" in digital format, including, but not limited to, objects containing or representing data types such as text, images, video, linear motion pictures in digital format, sound recordings and other audio information, computer software, smart agents, multimedia, and/or objects any combination of two or more data types contained within or representing a single compound object. Content (executables for example) delivered with proof of delivery and/or execution or other use. Secure electronic containers can be delivered. The containers can maintain control, audit, receipt and other information and protection securely and persistently in association with one or more items. Trustedness provides non-repudiation for legal and other transactions. Can handle and send any digital information (for example, analog or digital information representing text, graphics, movies, animation, images, video, digital linear motion pictures, sound and sound recordings, still images, software computer programs or program fragments, executables, data, and including multiple, independent pieces of text; sound clips, software for interpreting and presenting other elements of content, and anything else that is electronically representable). Provides automatic electronic mechanisms that associate transactions automatically with other transactions. System can automatically insert or embed a variety of visible or invisible "signatures" such as images of handwritten signatures, seals, and electronic "fingerprints" indicating who has "touched" (used or other interacted with in any monitorable manner) the item. System can affix visible seals on printed items such as documents for use both in encoding receipt and other receipt and/or usage related information and for establishing a visible presence and impact regarding the authenticity, and ease of checking the authenticity, of the item. Seals can indicate who originated, sent, received, previously received and redistributed, electronically view, and/or printed and/or otherwise used the item. Seals can encode digital signatures and validation information providing time, location, send and/or other information and/or providing means for item authentication and integrity check. Scanning and decoding of item seals can provide authenticity/integrity check of entire item(s) or part of an item (e.g., based on number of words, format, layout, image—picture and/or test—composition, etc.). Seals can be used to automatically associate electronic control sets for use in further item handling. System can hide additional information within the item using "stenanography" for later retrieval and analysis. Steganography can be used to encode electronic fingerprints and/or other information into an item to prevent deletion. Multiple stenanographic storage of the same fingerprint information may be employed reflecting "more" public and "less" public modes so that a less restricted steganographic mode (different encryption algorithm, keys, and/or embedding techniques) can be used to assist easy recognition by an authorized party and a more private (confidential) mode may be readable by only a few parties (or only one party) and comprise of the less restricted mode may not affect the security of the more private mode. Items such as documents can be electronically, optically scanned at the sender's end—and printed out in original, printed form at the recipient's end. Document handlers and processors can integrate document scanning and delivery. Can be directly integrated into enterprise and Internet (and similar network) wide document workflow systems and applications. Secure, tamper-resistant electronic appliance, which may employ VDE SPUs, used to handle items at both sender and recipient ends.

Claim Term	MS Construction
	"Original" item(s) can automatically be destroyed at the sender's end and reconstituted at the recipient's end to prevent two originals from existing simultaneously. Secure, non-repudiable authentication of the identification of a recipient before delivery using any number of different authentication techniques including but not limited to biometric techniques (such as palm print scan, signature scan, voice scan, retina scan, iris scan, biometric fingerprint and/or handprint scan, and/or face profile) and/or presentation of a secure identity "token." Non-repudiation provided through secure authentication used to condition events (e.g., a signature is affixed onto a document only if the system securely authenticates the sender and her intention to agree to its contents). Variety of return receipt options including but not limited to a receipt indicating who opened a document, when, where, and the disposition of the document (stored, redistributed, copied, etc.). These receipts can later be used in legal proceedings and/or other contexts to prove item delivery, receipt and/or knowledge. Audit, receipt, and other information can be delivered independently from item delivery, and become securely associated with an item within a protected processing environment. Secure electronic controls can specify how an item is to be processed or otherwise handled (e.g., document can't be modified, can be distributed only to specified persons, collections of persons, organizations, can be edited only by certain persons and/or in certain manners, can only be viewed and will be "destroyed" after a certain elapse of time or real time or after a certain number of handlings, etc.) Persistent secure electronic controls can continue to supervise item workflow even after it has been received and "read." Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility. Secure controls can be used in conjunction with digital electronic certificates certifying as to identity, class (age, organization membership, jurisdiction, etc.) of the sender and/or receiver and/or user of communicated information. Efficiently handles payment and electronic addressing arrangements through use of support and administrative services such as a Distributed Commerce Utility as more fully described in the copending Shear, et al. application. Compatible with use of smart cards, including, for example, VDE enabled smart cards, for secure personal identification and/or for payment. Transactions may be one or more component transactions of any distributed chain of handling and control process including Electronic Data Interchange (EDI) system, electronic trading system, document workflow sequence, and banking and other financial communication sequences, etc. ('683 6:18) - "Content providers and distributors have devised a number of limited function rights protection mechanisms to protect their rights. Authorization passwords and protocols, license servers, "lock/unlock" distribution methods, and non-electronic contractual limitations imposed on users of shrink-wrapped software are a few of the more prevalent content protection schemes. In a commercial context, these efforts are inefficient and limited solutions." ('900 2:64) - "The inability of conventional products to be shaped to the needs of electronic information providers and users is sharply in contrast to the present invention. Despite the attention devoted by a cross-section of America's largest telecommunications, computer, entertainment and information provider companies to some of the problems addressed by the present invention, only the present invention provides commercially secure, effective solutions for configurable, general purpose electronic commerce transaction/distribution control systems." ('193 2:13) - "The features of VDE allow it to function as the first trusted electronic information control environment that can conform to, and support, the bulk of conventional electronic commerce and data security requirements. In particular, VDE enables the participants in a business value chain model to create an electronic version of traditional business agreement terms and conditions and further enables these participants to shape and evolve their electronic commerce models as they believe appropriate to their business requirements." ('193 8:43)

Claim Term	MS Construction
	- An objective of VDE is supporting a transaction/distribution control standard. Development of such a standard has many obstacles, given the security requirements and related hardware and communications issues, widely differing environments, information types, types of information usage, business and/or data security goals, varieties of participants, and properties of delivered information. A significant feature of VDE accommodates the many, varying distribution and other transaction variables by, in part, decomposing electronic commerce and data security functions into generalized capability modules executable within a secure hardware SPU and/or corresponding software subsystem and further allowing extensive flexibility in assembling, modifying, and/or replacing, such modules (e.g. load modules and/or methods) in applications run on a VDE installation foundation. This configurability and reconfigurability allows electronic commerce and data security participants to reflect their priorities and requirements through a process of iteratively shaping an evolving extended electronic agreement (electronic control model). ('193 15:66)

- Some of the key factors contributing to the configurability intrinsic to the present invention include: (a) integration into the fundamental control environment of a broad range of electronic appliances through portable API and programming language tools that efficiently support merging of control and auditing capabilities in nearly any electronic appliance environment while maintaining overall system security; (b) modular data structures; (c) generic content model; (d) general modularity and independence of foundation architectural components; (e) modular security structures; (f) variable length and multiple branching chains of control; and (g) independent, modular control structures in the form of executable load modules that can be maintained in one or more libraries, and assembled into control methods and models, and where such model control schemes can "evolve" as control information passes through the VDE installations of participants of a pathway of VDE content control information handling. ('193 16:66)

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... provide mechanisms that allow control information to "evolve" and be modified according, at least in part, to independently, securely delivered further control information. ... Handlers in a pathway of handling of content control information, to the extent each is authorized, can establish, modify, and/or contribute to, permission, auditing, payment, and reporting control information related to controlling, analyzing, paying for, and/or reporting usage of, electronic content and/or appliances (for example, as related to usage of VDE controlled property content)." ('193 21:43, 29:21)

- "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... enable a user to securely extract, through the use of the secure subsystem at the user's VDE installation, at least a portion of the content included within a VDE content container to produce a new, secure object (content container), such that the extracted information is maintained in a continually secure manner through the extraction process." ('193 21:43 31:66)

- "As with the content control information for most VDE managed content, features of the present invention allows [sic] the content's control information to: (a) "evolve," for example, the extractor of content may add new control methods and/or modify control parameter data, such as VDE application compliant methods, to the extent allowed by the content's in-place control information. ... (b) allow a user to combine additional content with at least a portion of said extracted content, ... (c) allow a user to securely edit at least a portion of said content while maintaining said content in a secure form within said VDE content container; ... (d) append extracted content to a pre-existing VDE content container object and attach associated control information ... (e) preserve VDE control over one or more portions |

Claim Term	MS Construction
	of extracted content after various forms of usage of said portions ... Generally, the extraction features of the present invention allow users to aggregate and/or disseminate and/or otherwise use protected electronic content information extracted from content container sources while maintaining secure VDE capabilities thus preserving the rights of providers in said content information after various content usage processes." ('193 32:27) - The secure component based architecture of ROS 602 has important advantages. For example, it accommodates limited resource execution environments such as provided by a lower cost SPU 500. It also provides an extremely high level of configurability. In fact, ROS 602 will accommodate an almost unlimited diversity of content types, content provider objectives, transaction types and client requirements. In addition, the ability to dynamically assemble independently deliverable components at execution time based on particular objects and users provides a high degree of flexibility, ('193 87:63) - "Each logical object structure 800 may also include a "private body" 806 containing or referencing a set of methods 1000 (i.e., programs or procedures) that control use and distribution of the object 300. The ability to optionally incorporate different methods 1000 with each object is important to making VDE 100 highly configurable." ('193 128:25) - "VDE methods 1000 are designed to provide a very flexible and highly modular approach to secure processing." ('193 181:17) - "The reusable functional primitives of VDE 100 can be flexibly combined by content providers to reflect their respective distribution objectives." ('193 255:27) - the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment." ('193 261:12) - "Adding new content to objects is an important aspect of authoring provided by the present invention. Providers may wish to allow one or more users to add, hide, modify, remove and/or extend content that they provide. In this way, other users may add value to, alter for a new purpose, maintain, and/or otherwise change, existing content. The ability to add content to an empty and/or newly created object is important as well." ('193 261:23) - "The distribution control information provided by the present invention allows flexible positive control. No provider is required to include any particular control, or use any particular strategy, except as required by senior control information. Rather, the present invention allows a provider to select from generic control components (which may be provided as a subset of components appropriate to a provider's specific market, for example, as included in and/or directly compatible with, a VDE application) to establish a structure appropriate for a given chain of handling/control." ('193 297:9)"Importantly, VDE securely and flexibly supports editing the content in, extracting content from, embedding content into, and otherwise shaping the content composition of, VDE content containers. Such capabilities allow VDE supported product models to evolve by progressively reflecting the requirements of "next" participants in an electronic commercial model." ('193 297:9) - "For instance, the user may have an "access" right, and an "extraction" right, but not a "copy" right." ('193 159:24) - "PERCS 808 specify a set of rights that may be exercised to use or access the corresponding VDE object 300. The preferred embodiment allows users to "customize" their access rights by selecting a subset of rights authorized by a corresponding PERC 808 and/or by specifying parameters or choices that correspond to some or all of the rights granted by PERC 808. These user choices are set forth in a user rights table 464 in the preferred embodiment. User rights table (URT) 464 includes URT records, each of which correspond to a user (or group of users). Each of these URT records specific users choices for a corresponding VDE object more methods 1000 for exercising the rights granted to the user by the PERC 808 in a way specified by the choices contained within the URT record." ('193 156:55) - "PERC and URT structures provide a mechanism that may be used to provide precise electronic representation of rights and the controls associated with those rights. VDE thus provides a

Claim Term	MS Construction
	"vocabulary" and mechanism by which users and creators may specify their desires." ('193 245:10)

- "In sum, the present invention allows information contained in electronic information products to be supplied according to user specification. Tailoring to user specification allows the present invention to provide the greatest value to users, which in turn will generate the greatest amount of electronic commerce activity." ('193 22:66)

- Function: "Adding new content to objects is an important aspect of authoring provided by the present invention. Providers may wish to allow one or more users to add, hide, modify, remove and/or extend content that they provide. In this way, other users may add value to, alter for a new purpose, maintain, and/otherwise change, existing content. The ability to add content to an empty and/or newly created object is important as well." ('193 261:23)

- Function: "Each logical object structure 800 may also include a "private body" 806 containing or referencing a set of method 1000 (i.e., programs or procedures) that control use and distribution of the object 300. The ability to optionally incorporate different methods 1000 with each object is important to making VDE 100 highly configurable." ('193 128:25)

- Function: "An important aspect of adding or modifying content is the choice of encryption/decryption keys and/or other relevant aspects of securing new or altered content." ('193 262:21)

- Function: "Importantly, VDE securely and flexibly supports editing the content in, extracting content from, embedding content into, and otherwise shaping the content composition of, VDE content containers." ('193 297:9)

- VDE also features fundamentally important capabilities for managing content that travels "across" the "information highway." These capabilities comprise a rights protection solution that serves all electronic community members. These members include content creators and distributors, financial service providers, end-users, and others. VDE is the first general purpose, configurable, transaction control/rights protection solution for users of computers, other electronic appliances, networks, and the information highway." ('193 2:27)

- VDE provides a unified solution that allows all content creators, providers, and users to employ the same electronic rights protection solution. ('193 5:17)

- "Since different groups of components can be put together for different applications, the present invention can provide electronic control information for a wide variety of different products and markets. This means the present invention can provide a "unified," efficient, secure, and cost-effective system for electronic commerce and data security. This allows VDE to serve as a single standard for electronic rights protection, data security, and electronic currency and banking." ('193 7:6)

- "Employing VDE as a general purpose electronic transaction/distribution control system allows users to maintain a single transaction management control arrangement on each of their computers, networks, communication nodes, and/or other electronic appliances. Such a general purpose system can serve the needs of many electronic transaction management applications without requiring distinct, different installations for different purposes. As a result, users of VDE can avoid the confusion and expense and other inefficiencies of different, limited purpose transaction control applications for each different content and/or business model. For example, VDE allows content creators to use the same VDE foundation control arrangement for both content authoring and for licensing content from other content creators for inclusion into their products or for other use. Clearinghouses, distributors, content creators, and other VDE users can all interact, both with the applications running on their VDE installations, and with each other, in an entirely consistent manner, using and reusing (largely transparently) the same distributed tools, mechanisms, and consistent user interfaces, regardless of the type of VDE activity." ('193 11:38)

- An objective of VDE is supporting a transaction/distribution control standard. ('193 55:66)

- Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... The design of the VDE foundation, VDE load modules, and VDE containers, are important features that enable the VDE node operating environment to be compatible with a very broad |

Claim Term	MS Construction
	range of electronic appliances. The ability, for example, for control methods based on load modules to execute in very "small" and inexpensive secure sub-system environments, such as environments with very little read/write memory, while also being able to execute in large memory sub-systems that may be used in more expensive electronic appliances, supports consistency across many machines. This consistent VDE operating environment, including its control structures and container architecture, enables the use of standardized VDE content containers across a broad range of device types and host operating environments. Since VDE capabilities can be seamlessly integrated as extensions, additions, and/or modifications to fundamental capabilities of electronic appliances and host operating systems, VDE containers, content control information, and the VDE foundation will be able to work with many device types and these device types will be able to consistently and efficiently interpret and enforce VDE control information. ('193 ~~23:43~~ 34:26) - This rationalization stems from the reusability of control structures and user interfaces for a wide variety of transaction management related activities. As a result, content usage control, data security, information auditing, and electronic financial activities, can be supported with tools that are reusable, convenient, consistent, and familiar. In addition, a rational approach--a transaction/distribution control standard--allows all participants in VDE the same foundation set of hardware control and security, authoring, administration, and management tools to support widely varying types of information, business market model, and/or personal objectives ('193 11:26) - Because of the breadth of issues resolved by the present invention, it can provide the emerging "electronic highway" with a single transaction/distribution control system that can, for a very broad range of commercial and data security models, ensure against unauthorized use of confidential and/or proprietary information and commercial electronic transactions. VDE's electronic transaction management mechanisms can enforce the electronic rights and agreements of all parties participating in widely varying business and data security models, and this can be efficiently achieved through a single VDE implementation within each VDE participant's electronic appliance. VDE supports widely varying business and/or data security models that can involve a broad range of participants at various "levels" of VDE content and/or content control information pathways of handling. Different content control and/or auditing models and agreements may be available on the same VDE installation. These models and agreements may control content in relationship to, for example, VDE installations and/or users in general; certain specific users, installations, classes and/or other groupings of installations and/or users; as well as to electronic content generally on a given installation, to specific properties, property portions, classes and/or other groupings of content.('193 17:22) - "the present invention's trusted/secure, universe wide, distributed transaction control and administration system." ('193 35:66) - "Commerce Utility Systems 90 are generalized and programmable..." ('712 67:7) - "Providers of "electronic currency" have also created protections for their type of content. These systems are not sufficiently adaptable, efficient, nor flexible enough to support the generalized use of electronic currency. Furthermore, they do not provide sophisticated auditing and control configuration capabilities. This means that current electronic currency tools lack the sophistication needed for many real- world financial business models. VDE provides means for anonymous currency and for "conditionally" anonymous currency, wherein currency related activities remain anonymous except under special circumstances." ('193 3:10) - "Traditional content control mechanisms often require users to purchase more electronic information than the user needs or desires. For example, infrequent users of shrink-wrapped software are required to purchase a program at the same price as frequent users, even though they may receive much less value from their less frequent use. Traditional systems do not scale cost according to the extent or character of usage and traditional systems can not attract potential customers who find that a fixed price is too high. Systems using traditional mechanisms are also not normally particularly secure. For example, shrink-wrapping does not prevent the constant illegal pirating of software once removed from either its physical or electronic package." ('193 5:50) - "Traditional electronic information rights protection systems are often inflexible and inefficient and

Claim Term	MS Construction
	may cause a content provider to choose costly distribution channels that increase a product's price. In general these mechanisms restrict product pricing, configuration, and marketing flexibility. These compromises are the result of techniques for controlling information which cannot accommodate both different content models and content models which reflect the many, varied requirements, such as content delivery strategies, of the model participants. This can limit a provider's ability to deliver sufficient overall value to justify a given product's cost in the eyes of many potential users. VDE allows content providers and distributors to create applications and distribution networks that reflect content providers' and users' preferred business models. It offers users a uniquely cost effective and feature rich system that supports the ways providers want to distribute information and the ways users want to use such information." ('193 5:36)

- "VDE does not require electronic content providers and users to modify their business practices and personal preferences to conform to a metering and control application program that supports limited, largely fixed functionality [sic]. Furthermore, VDE permits participants to develop business models not feasible with non- electronic commerce, for example, involving detailed reporting of content usage information, large numbers of distinct transactions at hitherto infeasible low price points, "pass-along" control information that is enforced without involvement or advance knowledge of the participants, etc." ('193 9:67)

- "VDE can further be used to enable commercially provided electronic content to be made available to users in user defined portions, rather than constraining the user to use portions of content that were "predetermined" by a content creator and/or other provider for billing purposes." ('193 11:66)

- "The "usage map" concept provided by the preferred embodiment may be tied to the concept of "atomic elements." In the preferred embodiment, usage of an object 300 may be metered in terms of "atomic elements." In the preferred embodiment, an "atomic element" in the metering context defines a unit of usage that is "sufficiently significant" to be recorded in a meter. The definition of what constitutes an "atomic element" is determined by the creator of an object 300. For instance, a "byte" of information content contained in an object 300 could be defined as an "atomic element," or a record of a database could be defined as an "atomic element," or each chapter of an electronically published book could be defined as an "atomic element."" ('193 144:53)

- Summary of Some Important Features Provided by VDE in Accordance With the Present Invention. VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, VDE includes features that support dynamic user selection of information subsets of a VDE electronic information product (VDE controlled content). This contrasts with the constraints of having to use a few high level individual, pre-defined content provider information increments such as being required to select a whole information product or product section in order to acquire or otherwise use a portion of such product or section. VDE supports metering and usage control over a variety of increments (including "atomic" increments, and combinations of different increment types) that are selected ad hoc by a user and represent a collection of pre-identified one or more increments (such as one or more blocks of a preidentified nature, e.g., bytes, images, logically related blocks) that form a generally arbitrary, but logical to a user, content "deliverable." VDE control information (including budgeting, pricing and metering) can be configured so that it can specifically apply, as appropriate, to ad hoc selection of different, unanticipated variable user selected aggregations of information increments and pricing levels can be, at least in part, based on quantities and/or nature of mixed increment selections (for example, a certain quantity of certain text could mean associated images might be discounted by 15%; a greater quantity of text in the "mixed" increment selection might mean the images are discounted 20%). Such user selected aggregated information increments can reflect the actual requirements of a user for information and is more flexible than being limited to a single, or a few, high level, (e.g. product, document, database record) predetermined increments. Such high level increments may include quantities of information not desired by the user and as a result be more costly than the subset of information needed by the user if such a subset was available. In sum, the present invention allows information contained in electronic information products to be supplied according to user specification. Tailoring to user specification allows the present invention to provide |

Claim Term	MS Construction
	the greatest value to users, which in turn will generate the greatest amount of electronic commerce activity. The user, for example, would be able to define an aggregation of content derived from various portions of an available content product, but which, as a deliverable for use by the user, is an entirely unique aggregated increment. The user may, for example, select certain numbers of bytes of information from various portions of an information product, such as a reference work, and copy them to disc in unencrypted form and be billed based on total number of bytes plus a surcharge on the number of "articles" that provided the bytes. A content provider might reasonably charge less for such a user defined information increment since the user does not require all of the content from all of the articles that contained desired information. ('193 21:43, 22:32)

- Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... Differing models for billing, auditing, and security can be applied to the same piece of electronic information content and such differing sets of control information may employ, for control purposes, the same, or differing, granularities of electronic information control increments. ('193 21:43, 28:23))

- "The VDE templates, classes, and control structures are inherently flexible and configurable to reflect the breadth of information distribution and secure storage requirements, to allow for efficient adaptation into new industries as they evolve, and to reflect the evolution and/or change of an existing industry and/or business, as well as to support one or more groups of users who may be associated with certain permissions and/or budgets and object types. The flexibility of VDE templates, classes, and basic control structures is enhanced through the use of VDE aggregate and control methods which have a compound, conditional process impact on object control. Taken together, and employed at times with VDE administrative objects and VDE security arrangements and processes, the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment. Thus, the present invention fully supports the requirements and biases of content providers without forcing them to fit a predefined application model. It allows them to define the rights, control information, and flow of their content (and the return of audit information) through distribution channels." ('193 260:66)

- VDE also extends usage control information to an arbitrary granular level (as opposed to a file based level provided by traditional operating systems) and provides flexible control information over any action associated with the information which can be described as a VDE controlled process." ('193 275:8)

- "The situation is no better for processing documents within the context of ordinary computer and network systems. Although said systems can enforce access control information based on user identity, and can provide auditing mechanisms for tracking accesses to files, these are low-level mechanisms that do not permit tracking or controlling the flow of content. In such systems, because document content can be freely copied and manipulated, it is not possible to determine where document content has gone, or where it came from. In addition, because the control mechanisms in ordinary computer operating systems operate at a low level of abstraction, the entities they control are not necessarily the same as those that are manipulated by users. This particularly causes audit trails to be cluttered with voluminous information describing uninteresting activities." ('193 281:27)

- "Importantly, VDE securely and flexibly supports editing the content in, extracting content from, embedding content into, and otherwise shaping the content composition of, VDE content containers." ('193 297:9)

- "The InterTrust DigiBox container model allows and facilitates these and other different container uses. It facilitates detailed container customization for different uses, classes of use and/or users in order to meet different needs and business models. This customization ability is very important, particularly when used in conjunction with a general purpose, distributed rights management environment such as described in Ginter, et al. Such an environment calls for a practical optimization of customizability, including customizability and transparency for container models. This customization flexibility has a number of advantages, such as allowing optimization (e.g., maximum efficiency, minimum overhead) of the detailed container design for each particular application or circumstance so as to allow many different container designs for many different purposes (e.g., business models) to exist

Claim Term	MS Construction
	at the same time and be used by the rights control client (node) on a user electronic appliance such as a computer or entertainment device." ('861 2:49) - "The node and container model described above and in the Ginter et al. patent specification (along with similar other DigiBox/VDE (Virtual Distribution Environment) models) has nearly limitless flexibility." ('861 2:37) Such capabilities allow VDE supported product models to evolve by progressively reflecting requirements of "next" participants in an electronic commercial models." ('193 297:12) Extrinsic: VDE: VDE is the broad name given to a comprehensive system (algorithms, software, and hardware) that provides metering, securing, and administration tools for intellectual property. VDE stands for "Virtual Distribution Environment." (VDE ROI DEVICE v1.0a 9 Feb 1994, IT00008570) Virtual: Pertaining to a functional unit that appears to be real, but whose functions are accomplished by other means.(IBM) Environment: 1. The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system. 2. In computer security, those factors, both internal and external, of an ADP system that help to define the risks associated with its operation (Longley) Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment*. (ITG, 8/21/95, IT00032375, TD00068B) InterTrust Commerce Architecture model: A model that defines a general-purpose distributed architecture for secure electronic commerce and digital rights management. The InterTrust Commerce Architecture model includes four key software elements: DigiBox secure containers, InterRights Point software with associated protected database, the InterTrust Transaction Authority Framework, and the InterTrust Deployment Manager. (ITG, 1997, ML00012A) VDE is a system using secure computing technology to enforce a chain of handling and control representing the rights of interested parties. (ITG, 3/7/1995, IT00709616) (see footnote 2) Virtual Distribution Environment (VDE): A set of components that protects content and enforces rights associated with content. (ITG, 3/7/1995, IT00709620, see footnote 2) Virtual Distribution Environment: or "VDE" shall mean a system which guarantees: (I) that the content creators, publishers, and/or distributors of information receive agreed upon fees for the use of, and/or records of the use of, electronic content; and/or (ii) that stored and/or distributed information will be used only in authorized ways. More particularly, VDE relates to systems for applying controls to, and controlling and/or auditing use of, electronically stored and/or disseminated information. [License Agreement, National Semiconductor and EPR, 3/18/94, Exhibit 12 to IT 30(b)(6)) IT0001689-96, IT0709785 (VDE on a Page), IT000202-29
'193:1	"The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
receiving a digital file including music	Intrinsic: - "Moreover, when any new VDE object 300 arrives at an electronic appliance 600, the electronic appliance must "register" the object within object registry 450 so that it can be accessed." ('193 153:56) - "FIGS. 114A and 114B show an example process 4600 for receiving an item. In this example,

Claim Term	MS Construction
	electronic appliance 600 that has received an electronic object 300 may first generate a notification to PPE 650 that the container has arrived (FIG. 114A, block 4602). PPE 650 may, in response, use the dynamic user interaction techniques discussed above to interact with and authenticate the recipient in accordance with the electronic controls 4078 within the received object 300 (FIG. 114A block 4603; authentication routine shown in FIG. 111). Intended recipient 4056 may be given an option of accepting or declining delivery of the object (FIG. 114A, block 4604). If intended recipient 4056 accepts the item, appliance may store the container 302 locally (FIG. 114A, block 4606) and then generate a "register object" event for processing by PPE 650." - while grandparent ('107) did not refer to fax transmission or physical mail, it did recite that the delivery means could be by "physical storage media" or by transferring "physical things" ('193 3:26, 5:4, 14:21, 18:10, 127:6, 242:32) "In this example, the trusted electronic go-between between 4700 receives notification that the electronic container 302 has arrived (FIG. 121, block 4752), may store the container locally (FIG. 121, block 4754), and opens and authenticates the container and its contents (FIG. 121, block 4756). The trusted electronic go-between 4700 may then, if necessary, obtain and locally register any method/rules required to intract with secure container 302 (FIG. 121, block 4758)." Extrinsic:
a budget specifying the number of copies which can be made of said digital file	Intrinsic: - For example, content control information for a given piece of content may be stipulated as senior information and therefore not changeable, might be put in place by a content creator and might stipulate that national distributors of a given piece of their content may be permitted to make 100,000 copies per calendar quarter, so long as such copies are provided to bonfire end-users, but may pass only a single copy of such content to a local retailers and the control information limits such a retailer to making no more than 1,000 copies per month for retail sales to end-users. In addition, for example, an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer). ('193 48:19) - "storing a first digital file and a first control in a first secure container, said first control constituting a first budget which governs the number of copies which may be made of said first digital file or a portion of said first digital file while said first digital file is contained in said first secure container," ('193 claim 60) - "A certain content provider might, for example, require metering the number of copies made for distribution to employees of a given software program (a portion of the program might be maintained in encrypted form and require the presence of a VDE installation to run). This would require the execution of a metering method for copying of the property each time a copy was made for another employee." ('193 20:36) - For example, in the earlier example of a user with a desktop and a notebook computer, a provider may allow a user to make copies of information necessary to enable the notebook computer based on information present in the desktop computer, but not allow any further copies of said information to be made by the notebook VDE node. In this example, the distribution control structure described earlier would continue to exist on the desktop computer, but the copies of the enabling information passed to the notebook computer would lack the required distribution control structure to perform distribution from the notebook computer. Similarly, a distribution control structure may be provided by a content provider to a content provider who is a distributor in which a control structure would enable a certain number of copies to be made of a VDE content container object along with associated copies of permissions records, but the permissions records would be altered (as per specification of the content provider, for example) so as not to allow end-users who received distributor created copies from making further copies for distribution to other VDE nodes.('193 264:29) - "Similarly, a distribution control structure may be provided ... so as not to allow end-users who received distributor created copies from making further copies for distribution to other VDE nodes."

Claim Term	MS Construction
	('193 264:40) - SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. ('193 59:48) - " Secure container 302 may also contain an electronic, digital control structure 4078. This control structure 4078 (which could also be delivered independently in another container 302 different from the one carrying the image 4068I and/or the data 4068D) may contain important information controlling use of container 302. For example, controls 4078 may specify who can open container 302 and under what conditions the container can be opened. Controls 4078 might also specify who, if anyone, object 300 can be passed on to. As another example, controls 4078 might specify restrictions on how the image 4068I and/or data 4068D can be used (e.g., to allow the recipient to view but not change the image and/or data as one example). The detailed nature of control structure 4078 is described in connection, for example, with FIGS. 11D-11J ; FIG. 15 ; FIGS. 17-26B; and FIGS. 41A-61 ." ('683 25:62)"Many objects 300 that are distributed by physical media and/or by "out of channel" means (e.g., redistributed after receipt by a customer to another customer) might not include key blocks 810 in the same object 300 that is used to transport the content protected by the key blocks. This is because VDE objects may contain data that can be electronically copied outside the confines of a VDE node. If the content is encrypted, the copies will also be encrypted and the copier cannot gain access to the content unless she has the appropriate decryption key(s)." ('193 128:66) Although block 1262 includes encrypted summary services information on the back up, it preferably does not include SPU device private keys, shared keys, SPU code and other internal security information to prevent this information from ever becoming available to users even in encrypted form. ('193 166:59) Extrinsic:
controlling the copies made of said digital file	See above.
determining whether said digital file may be copied and stored on a second device based on at least said copy control	Intrinsic: - "Similarly, a distribution control structure may be provided ... so as not to allow end-users who received distributor created copies from making further copies for distribution to other VDE nodes." ('193 264:40) - "As mentioned above, traveling objects enable objects 300 to be distributed "Out-Of-Channel;" that is, the object may be distributed by an unauthorized or not explicitly authorized individual to another individual. "Out of channel" includes paths of distribution that allow, for example, a user to directly redistribute an object to another individual. For example, an object provider might allow users to redistribute copies of an object to their friends and associates (for example by physical delivery of storage media or by delivery over a computer network) such that if a friend or associate satisfies any certain criteria required for use of said object, he may do so." ('193 131:53) - "In some cases, the extract rights require an exact copy of the PERC 808 associated with the original object (or a PERC included for this purpose) to be placed in the new (destination) container ("no" exit to decision block 2096)." ('193 194:47) - "Metering, billing, and budgeting can allow a provider to enable and limit the copying of a permissions record 808." ('193 263:54) - "In some circumstances, it may be desirable for a provider to control how administrative processes are performed. The provider may choose to include in distribution records stored in secure database 610 information for use in conjunction with a component assembly 690 that controls and specifies, for example, how processing for a given event in relation to a given method and/or record should be performed. For example, if a provider wishes to allow a user to make copies of a permissions record

Claim Term	MS Construction
	808, she may want to alter the permissions record internally. For example, in the earlier example of a user with a desktop and a notebook computer, a provider may allow a user to make copies of information necessary to enable the notebook computer based on information present in the desktop computer, but not allow any further copies of said information to be made by the notebook VDE node. In this example, the distribution control structure described earlier would continue to exist on the desktop computer, but the copies of the enabling information passed to the notebook computer would lack the required distribution control structure to perform distribution from the notebook computer. Similarly, a distribution control structure may be provided by a content provider to a content provider who is a distributor in which a control structure would enable a certain number of copies to be made of a VDE content container object along with associated copies of permissions records, but the permissions records would be altered (as per specification of the content provider, for example) so as not to allow end-users who received distributor created copies from making further copies for distribution to other VDE nodes." ('193 264:20) "Transfer of ownership of a VDE object 300 is a special case in which all of the permissions and/or budgets for a VDE object are redistributed to a different PPE 650. Some VDE objects may require that all object-related information be delivered (e.g., it's possible to "sell" all rights to the object). However, some VDE objects 300 may prohibit such a transfer." ('193 220:41) Extrinsic:
if said copy control allows at least a portion of said digital file to be copied and stored on a second device	Intrinsic: - "Persistence of control includes the ability to extract information from a VDE container object by creating a new container whose contents are at least in part secured and that contains both the extracted content and at least a portion of the control information which control information of the original container and/or are at least in part produced by control information of the original container for this purpose and/or VDE installation control information stipulates should persist and/or control usage of content in the newly formed container." ('193 28:50) "enable a user to securely extract, through the use of the secure subsystem at the user's VDE installation, at least a portion of the content included within a VDE content container to produce a new, secure object (content container), such that the extracted information is maintained in a continually secure manner through the extraction process. Formation of the new VDE container containing such extracted content shall result in control information consistent with, or specified by, the source VDE content container, and/or local VDE installation secure subsystem as appropriate, content control information. Relevant control information, such as security and administrative information, derived, at least in part, from the parent (source) object's control information, will normally be automatically inserted into a new VDE content container object containing extracted VDE content. This process typically occurs under the control framework of a parent object and/or VDE installation control information executing at the user's VDE installation secure subsystem (with, for example, at least a portion of this inserted control information being stored securely in encrypted form in one or more permissions records)." ('193 31:66) Extrinsic:
copying at least a portion of said digital file	Intrinsic: "Usage map meters are thus an efficient means for referencing prior usage. They may be used to enable certain VDE related security functions such as testing for contiguousness (including relative contiguousness), logical relatedness (including relative logical relatedness), usage randomization, and other usage patterns. For example, the degree or character of the "randomness" of content usage by a user might serve as a potential indicator of attempts to circumvent VDE content budget limitations. A user or groups of users might employ multiple sessions to extract content in a manner which does not violate contiguousness, logical relatedness or quantity limitations, but which nevertheless enables reconstruction of a material portion or all of a given, valuable unit of content. Usage maps can be

Claim Term	MS Construction
	analyzed to determine other patterns of usage for pricing such as, for example, quantity discounting after usage of a certain quantity of any or certain atomic units, or for enabling a user to reaccess an object for which the user previously paid for unlimited accesses (or unlimited accesses over a certain time duration). Other useful analyses might include discounting for a given atomic unit for a plurality of uses." ('193 146:54) Extrinsic:
transferring at least a portion of said digital file to a second device	Intrinsic: - "In this case, these users may still be able to transfer some or all usage rights to another electronic appliance 600, and/or they may be permitted to move some of their rights to another electronic appliance, if such transferring and/or moving is permitted by the usage permissions received from the repository 200g." ('193 317:12) - "A result of processing the distribute event within the BUDGET method might be a secure communication (1454) between VDE nodes 102 and 106 by which a budget granting use and redistribute rights to the distributor 106 may be transferred from the creator 102 to the distributor." ('193 173:1) "VDE securely managed content (e.g. through the use of a VDE aware application or operating system having extraction capability) may be identified for extraction from each of one or more locations within one or more VDE content containers and may then be securely embedded into a new or existing VDE content container through processes executing VDE controls in a secure subsystem PPE 650." ('193 301:26) Extrinsic:
storing said digital file	See above.
'193:11	Intrinsic: "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
receiving a digital file	See above.
determining whether said digital file may be copied and stored on a second device based on said first control	See above.
identifying said second device	See above.
whether said first control allows	See above.

EXHIBIT D TO JOINT CLAIM CONSTRUCTION STATEMENT- Page 78 of 100

Claim Term	MS Construction
transfer of said copied file to said second device	
said determination based at least in part on the features present at the device	Intrinsic: - "The software-based tamper resistant barrier 674 provided by HPE 655 may be provided, for example, by: ... using a map of defects on a storage device (e.g., a hard disk, memory card, etc.) to form internal test values to impede moving and/or copying HPE 655 to other electronic appliances 600" ('193 80:40) "The degree of trustedness of a VDE arrangement will be primarily based on whether hardware SPUs are employed at participant location secure subsystems and the effectiveness of the SPU hardware security architecture, software security techniques when an SPU is emulated in software, and the encryption algorithm(s) and keys that are employed for securing content, control information, communications, and access to VDE node (VDE installation) secure subsystems." ('193 45:52) - "Independent claim 122 recites "determining step including identifying said second device and determining whether said first control allows transfer of said copied file to said device, said determination based at least in part on the features present at the device to which said copied file is to be transferred" which distinguishes over Löfberg which provides for determination of the identification of a second device (the user station) but dies [sic] not provide for basing the determination at least in part on the features present at the device to which the copied file is to be transferred." "At the terminal TERM the personal data carrier ID is used for the input of customer identification information, for example an account number or a corresponding information. Simultaneously, the time of rent and a programme identification information is supplied to the terminal." (Löfberg, U.S. Pat. No. 4,595,950, 12:51-56) 09/208,017 ('193), Examiner's Supplemental Notice of Allowability, 11/06/00, p. 2 (MSI026638) Extrinsic:
if said first control allows at least a portion of said digital file to be copied and stored on a second device	See above.
copying at least a portion of said digital file	See above.
transferring at least a portion of said digital file to a second device	See above.
storing said digital file	See above.
'193:15	"The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2

Claim Term	MS Construction
	See "Virtual Distribution Environment" above.
receiving a digital file	See above.
an authentication step comprising:	Intrinsic: "The secure subsystems at said user nodes utilize a protocol that establishes and authenticates each node's and/or participant's identity" ('193 12:35) Extrinsic:
accessing at least one identifier associated with a first device or with a user of said first device	Intrinsic: - "a stipulation that the traveling object may be used on certain one or more installations or installation classes or users or user classes where classes correspond to a specific subset of installations or users who are represented by a predefined class identifiers stored in a secure database 610" ('193 131:40) - "Thus, if the user had a VDE node, the user might be able to use the traveling object ... if he or his VDE node belonged to a specially authorized group of users or installations" ('193 132:13) - "A traveling object might register its user within itself and thereafter only be useable by that one user." ('193 133:43) - "Administrative objects, for example, may increase or otherwise adjust budgets and/or permissions of the receiving VDE node to which the administrative object is being sent." ('193 135:21) - "This metering process may ... record the VDE node name, user name, associated object identification information, time, date, and/or other identification information. Some or all of this information can become part of audit information securely reported by a clearinghouse or distributor.... For each metered one or more permissions records (or set of records) that were created for a certain user (and/or VDE node) to manage use of certain one or more VDE object(s) and/or to manage the creation of VDE object audit reports, it may be desirable that an auditor receive corresponding audit information incorporated into an, at least in part, encrypted audit report." ('193 273:58) - "provide very flexible and extensible user identification according to individuals, installations, by groups such as classes" ('193 25:31). "During the same or different communication session, the terminal could similarly, securely communicate back to the portable appliance 2600 VDE secure subsystem details as to the retail transaction (for example, what was purchased and price, the retail establishment's digital signature, the retail terminal's identifier, tax related information, etc.)." ('193 233:35) Extrinsic: "User Authentication: The [Database Management System] can require rigrous user authentication. For example, a DBMS might require a user to pass both specific password and time-of-day checks." (Pfleeger, p.307)
determining whether said identifier is associated with a device and/or user authorized to store said digital file	See above.

storing said digital file in a first secure memory of said first device, but	Intrinsic:
	
	Claims 91 and 132, as added with this Preliminary Amendment
	    "91. A method comprising:
	      receiving a digital file;

Claim Term	MS Construction

only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized	storing said digital file in a first secure memory of a first device;
	    storing information associated with said digital file in a secure database stored on said first device, said information including at least one control;
	    determining whether said digital file may be copied and stored on a second device based on said at least one control;
	    if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,
	    copying at least a portion of said digital file;
	    transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;
	    storing said digital file in said memory of said second device; and
	    rendering said digital file through said output."
	"132. A method as in claim 91, further comprising:
	    an authentication step occurring prior to said step of storing said digital file in said memory of said first device, said authentication step comprising:
	    accessing at least one identifier associated with said first device or with a user of said first device;
	    determining whether said identifier is associated with a device and/or user authorized to store said digital file; and
	    proceeding with said storing step if said device and/or user is so authorized, but not proceeding with said step if said device and/or user is not authorized."
	
	09/208,017 ('193), Preliminary Amendment, 12/09/98, p. 1-2, 12
	
	"Claims ... 132-134 ... are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims."
	
	09/208,017 ('193), Office Action, 06/07/00, p. 4-5
	
	- "132. (Amended) A method [as in claim 91, further] comprising:
	    receiving a digital file;
	    an authentication step [occurring prior to said step of storing said digital file in said memory of said first device, said authentication step] comprising:
	    accessing at least one identifier associated with a [said] first device or with a user of said first device; and
	    determining whether said identifier is associated with a device and/or user authorized to store said digital file; [and proceeding with said storing step];
	    storing said digital file in a first secure memory of said first device, but only [proceeding with said storing step] if said device and/or user is so authorized, but not proceeding with said storing [step] if said device and/or user is not authorized;
	    storing information associated with said digital file in a secure database stored on said first device, said information including at least one control;
	    determining whether said digital file may be copied and stored on a second device based on said at least one control;
	    if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,
	    copying at least a portion of said digital file;
	    transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;
	    storing said digital file in said memory of said second device; and
	    rendering said digital file through said output."
	(pg. 5-6)
	"The examiner also objected to claims ... 132-134, ... as dependent upon a rejected base claim (OA, ¶5). With this Amendment, Applicants have amended the above-mentioned claims to an independent form including all the limitations of the rejected base claim and any intervening claims per the Examiner's suggestion."

Claim Term	MS Construction
	(pg. 22) 09/208,017 ('193), Amendment, 08/04/00, p. 5-6, 22 Extrinsic:
storing information associated with said digital file in a secure database stored on said first device, said information including at least one control	See above.
determining whether said digital file may be copied and stored on a second device based on said at least one control	See above.
if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,	See above.
copying at least a portion of said digital file	See above.
transferring at least a portion of said digital file to a second device	See above.
storing said digital file	See above.
'193:19	Intrinsic: "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
receiving a digital file at a first device	See above.

Claim Term	MS Construction
establishing communication between said first device and a clearinghouse located at a location remote from said first device	**Intrinsic:** "A usage clearinghouse 200c as described above in connection with FIG. 1A and/or as disclosed in the Shear et al. patent disclosure may be used to track the audit information based on event-driven or periodic reporting, for example. Audit records could be transmitted to a usage clearinghouse (or to a trusted go-between 4700) by an automatic call forwarding transmission, by a supplement call during transmission, by period update of audit information, by the maintenance of a constant communication line or open network pathway, etc." ('683 37:56) **Extrinsic:**
using said authorization information to gain access to or make at least one use of said first digital file	See above.
receiving a first control from said clearinghouse at said first device	See above.
storing said first digital file in a memory of said first device	See above.
using said first control to determine whether said first digital file may be copied and stored on a second device	See above.
if said first control allows at least a portion of said first digital file to be copied and stored on a second device	See above.
copying at least a portion of said first digital file	See above.
transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output	See above.
storing said first	See above.

Claim Term	MS Construction
digital file portion	
'683:2	Intrinsic: "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above. - Prosecution History of '683 Patent: "A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. ... claim 7 recites hardware and/or software used for transmission of secure containers to other apparatuses and/or for the receipt of secure containers from other apparatuses, see column 1, lines 18-24 and column 4, lines 58-69." 09/221,479 ('683), Office Action, 11/12/99, 4-5 (IT00065800-01) - Fischer, U.S. Pat. No. 5,412,717 : "Each terminal, A, B ... N also includes a conventional IBM communications board (not shown) which when coupled to a conventional modem 6, 8, 10, respectively, permits the terminals to transmit and receive messages. Each terminal is capable of generating a message performing whatever digital signature operations may be required and transmitting the message to any of the other terminals connected to communications channel 12 (or a communications network (not shown), which may be connected to communications channel 12)." (4:58-69)
the first secure container having been received from a second apparatus	Intrinsic: - "Incoming administrative object manager 756 typically maintains records (in concert with SPE 503) in secure database 610 (e.g., receiving table 446) that record which objects have been received, objects expected for receipt, and other information related to received and/or expected objects." ('193 102:46) - REGISTER method 2400 in this "administrative response" mode may prime appropriate audit trails (blocks 2460, 2462), and then may unpack the received administrative object and write the associated register request(s) configuration information into the secure database (blocks 2464, 2466). REGISTER method 2400 may then retrieve the administrative request from the secure database and determine which response method to run to process the request (blocks 2468, 2470). If the user fails to provide sufficient information to register the object, REGISTER method 2400 may fail (blocks 2472, 2474). ('193 179:23) - "Referring to FIG. 110, appliance 600 may then deliver the secure container(s) 302 to the intended recipient 4056 and/or to trusted electronic go-between 4700 based upon the instructions of sender 4052 as now reflected in the electronic controls 4078 associated with the object 300 (FIG. 110, block 4514). Such delivery is preferably by way of electronic network 4058 (672), but may be performed by any convenient electronic means such as, for example, Internet, Electronic Mail or Electronic Mail Attachment, WEB Page Direct, Telephone, floppy disks, bar codes in a fax transmission, filled ovals on a form delivered through physical mail, or any other electronic means to provide contact with the intended recipient(s)." ('683 40:10) Extrinsic:
an aspect of access to or use of	See above.

Claim Term	MS Construction
the first secure container rule having been received from a third apparatus different from said second apparatus	**Intrinsic:** "[A]pplicants' independent claims ... require secure delivery of <u>both</u> first <u>and</u> second control items originating from someplace <u>other</u> than the appliance where they are used, at least in part, for controlling the same process, operation or the like. This feature in combination is not taught or suggested by Johnson and/or Rosen." 08/388,107, Amendment, 06/20/97, p. 23 (MSI028847) - "Appliance 600 may next, if necessary, obtain and locally register any methods, controls or other information required to manipulate object 300 or its contents (FIG. 115, block 4607B; see registration method shown in FIGS. 43a-d). For example, item 4054 may be delivered independently of an associated control set 4078, where the control set may only be partial, such that appliance 600 may require additional controls from permissioning agent 200f (see FIG. 1A and "rights and permissions clearing house" description in the copending Shear et al. patent disclosure) or other archive in order to use the item." ('683 41:4) - "Secure container 302 may also contain an electronic, digital control structure 4078. This control structure 4078 (which could also be delivered independently in another container 302 different from the one carrying the image 4068I and/or the data 4068D) may contain important information controlling use of container 302." ('683 25:62) **Extrinsic:**
hardware or software used for receiving and opening secure containers	**Intrinsic:** "Please ... add the following new claims: 7. A system including, ... hardware and/or software used for receiving and opening secure containers ..." 09/221,479 ('683), Preliminary Amendment, 12/28/98, p. 2 - "SPU 500 in this example is an integrated circuit ("IC") "chip" 504 including "hardware" 506 and "firmware" 508. SPU 500 connects to the rest of the electronic appliance through an "appliance link" 510. SPU "firmware" 508 in this example is "software" such as a "computer program(s)" "embedded" within chip 504. Firmware 508 makes the hardware 506 work. Hardware 506 preferably contains a processor to perform instructions specified by firmware 508. "Hardware" 506 also contains long-term and short-term memories to store information securely so it can't be tampered with. SPU 500 may also have a protected clock/calendar used for timing events. The SPU hardware 506 in this example may include special purpose electronic circuits that are specially designed to perform certain processes (such as "encryption" and "decryption") rapidly and efficiently." ('193 59:60) - "Referring to FIG. 110, appliance 600 may then deliver the secure container(s) 302 to the intended recipient 4056 and/or to trusted electronic go-between 4700 based upon the instructions of sender 4052 as now reflected in the electronic controls 4078 associated with the object 300 (FIG. 110, block 4514). Such delivery is preferably by way of electronic network 4058 (672), but may be performed by any convenient electronic means such as, for example, Internet, Electronic Mail or Electronic Mail Attachment, WEB Page Direct, Telephone, floppy disks, bar codes in a fax transmission, filled ovals on a form delivered through physical mail, or any other electronic means to provide contact with the intended recipient(s)." ('683 40:10) - while grandparent ('107) did not refer to fax transmission or physical mail, it did recite that the delivery means could be by "physical storage media" or by transferring "physical things" ('193, 3:28, 5:4, 14:21, 18:10, 53:33, 127:6, 245:32) - "Incoming administrative object manager 756 receives administrative objects from other VDE electronic appliances 600 via communications manager 776." ('193 102:42)

Claim Term	MS Construction
	- Trusted go-between 4700 might be authorized to register (but not open) the containers 302(1) it receives for later use as evidence in court 5016. ('683 52:35) 479.7: "hardware and or/ [sic, and/or] software" Extrinsic:
said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers	Intrinsic: "VDE object creation in the preferred embodiment employs VDE templates whose atomic elements represent at least in part modular control processes. Employing VDE creation software (in the preferred embodiment a GUI programming process) and VDE templates, users may create VDE objects 300 by, for example, partitioning the objects, placing "meta data" (e.g., author's name, creation date, etc.) into them, and assigning rights associated with them and/or object content to, for example, a publisher and/or content creator. When a object creator runs through this process, she normally will go through a content specification procedure which will request required data. The content specification process, when satisfied, may be proceed by, for example, inserting data into a template and encapsulating the content." ('193 259:37) Extrinsic:
protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus	Intrinsic: See "protected processing environment" for Prosecution History limitations. "Such documents may be handled by people (referred to as "users") and/or by computers operating on behalf of users." ('193 277:36)" Extrinsic:
hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container	Intrinsic: - Prosecution History of '683 Patent: "A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. ... The combination of the first rule and the rule associated with the secure container is discussed at column 17, lines 40-61." U.S. Pat. No. 5,412,717 17:40-51: "Thereafter, the program X's program authorizing information is combined, as appropriate, with the PAI associated with the PCB of the calling program, if any. This combined PAI, which may include multiple PAI's, is then stored in an area of storage which cannot generally be modified by the program and the address of the PAI is stored in the process control block (PCB) as indicated in field 156 of FIG. 5. Thus, if program X is called by a calling program, it is subject to all its own constraints as well as being combined in some way with the constraints of the calling program, which aggregate constraints are embodied into program X's PAI." "A permissions record 808 may include requirements associated with this control information in combination with other control information, or a separate permissions record 808 may be used." ('193 262:17) 09/221,479 ('683), Office Action, 11/12/99, 4-5 (IT00065800-01)

Claim Term	MS Construction
	- "The VDE content control architecture allows content control information (such as control information for governing content usage) to be shaped to conform to VDE control information requirements of multiple parties. Formulating such multiple party content control information normally involves securely deriving control information from control information securely contributed by parties who play a role in a content handling and control model (e.g. content creator(s), provider(s), user(s), clearinghouse(s), etc.). Multiple party control information may be necessary in order to combine multiple pieces of independently managed VDE content into a single VDE container object (particularly if such independently managed content pieces have differing, for example conflicting, content control information). Such secure combination of VDE managed pieces of content will frequently require VDE's ability to securely derive content control information which accommodates the control information requirements, including any combinatorial rules, of the respective VDE managed pieces of content and reflects an acceptable agreement between such plural control information sets." ('193 296:12) - "The role of go-between 4700 may, in some circumstances, be played by one of the participant's SPU's 500 (PPEs), since SPU (PPE) behavior is not under the user's control, but rather can be under the control of rules and controls provided by one or more other parties other than the user (although in many instances the user can contribute his or her own controls to operate in combination with controls contributed by other parties)." ('683 24:26) - "Many such load modules are inherently configurable, aggregatable, portable, and extensible and singularly, or in combination (along with associated data), run as control methods under the VDE transaction operating environment." ('193 25:48) - "A permissions record 808 may include requirements associated with this control information in combination with other control information, or a separate permissions record 808 may be used." ('193 262:17) - "Seniority of contributed control information, including resolution of conflicts between content control information submitted by multiple parties, is normally established by:..." ('193 46:30) - "This attribute of supporting multiple party securely, independently deliverable control information is fundamental to enabling electronic commerce, that is, defining of a content and/or appliance control information set that represents the requirements of a collection of independent parties such as content creators, other content providers, financial service providers, and/or users." ('193 84:10) - "A significant feature of VDE accommodates the many, varying distribution and other transaction variables by, in part, decomposing electronic commerce and data security functions into generalized capability modules executable within a secure hardware SPU and/or corresponding software subsystem and further allowing extensive flexibility in assembling, modifying, and/or replacing, such modules (e.g. load modules and/or methods) in applications run on a VDE installation foundation. This configurability and reconfigurability allows electronic commerce and data security participants to reflect their priorities and requirements through a process of iteratively shaping an evolving extended electronic agreement (electronic control model). This shaping can occur as content control information passes from one VDE participant to another and to the extent allowed by "in place" content control information. This process allows users of VDE to recast existing control information and/or add new control information as necessary (including the elimination of no longer required elements)." ('193 16:5) - "A significant facet of the present invention's ability to broadly support electronic commerce is its ability to securely manage independently delivered VDE component objects containing control information (normally in the form of VDE objects containing one or more methods, data, or load module VDE components). This independently delivered control information can be integrated with senior and other pre-existing content control information to securely form derived control information using the negotiation mechanisms of the present invention. All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used. This means that, for example, all load modules and any mediating data which are listed by the derived control information as required must be available and securely perform their required function." ('193 10:66) - "Embedding takes content that is already in a container and stores it (or the complete object) in another container directly and/or by reference, integrating the control information associated with existing content with those of the new content." ('193 194:24)

Claim Term	MS Construction
⋮	- However, the EMBED method 2110 performs a slightly different function-it writes an object (or reference) into a destination container. Blocks 2112-2122 shown in FIG. 57b are similar to blocks 2082-2092 shown in FIG. 57a. At block 2124, EMBED method 2110 writes the source object into the destination container, and may at the same time extract or change the control information of the destination container. One alternative is to simply leave the control information of the destination container alone, and include the full set of control information associated with the object being embedded in addition to the original container control information. As an optimization, however, the preferred embodiment provides a technique whereby the control information associated with the object being embedded are "abstracted" and incorporated into the control information of the destination container. ('193 195:3) - Users of VDE may include content creators who apply content usage, usage reporting, and/or usage payment related control information to electronic content and/or appliances for users such as end-user organizations, individuals, and content and/or appliance distributors. ('193 9:40) - For example, in a VDE aware word processor application, a user may be able to "print" a document into a VDE content container object, applying specific control information by selecting from amongst a series of different menu templates for different purposes (for example, a confidential memo template for internal organization purposes may restrict the ability to "keep," that is to make an electronic copy of the memo). ('193 26:59) - '479 c. 7: "hardware and/or software used for" - "Collection of terms (a control set) define a contract associated with a specific right," ('193 245:56) - "securely combining said first and second controls to form a set of controls." ('107 pg. 733 claim 45) - "the right to use the content may be associated with two control sets. One control set may describe a fixed ("higher") price for using the content. Another control set may describe a fixed ("lower") price for using the content with additional content information and field specification requiring collection and return the user's personal information." ('193 246:50) - "Multiple party control information may be necessary in order to combine multiple pieces of independently managed VDE content into a single VDE container object (particularly if such independently managed content pieces have differing, for example, conflicting, content control information). Such secure combinations of VDE managed pieces of content will frequently require VDE's ability to securely derive content control information which accommodates the control information requirements, including any combinatorial rules, of the respective VDE managed pieces of content and reflects an acceptable agreement between such plural control information sets."('193 296:21) - "Control sets 914, in turn, each includes a control set header 916, a control method 918, and one or more require methods records 920." ('193 150:24) - "Each control set 914 contains as many required methods records 920 as necessary to satisfy all of the requirements of the creators and/or distributors for the exercise of a right." ('193 150:51) "Control sets 914 exist in two type in VDE 100: common required control sets which are given designations, "control sets 0" or "control set for right," and a set of control set options. "Control set 0" 902 contain a list of reuired methods that are common to all control set options, so that the common required methods do not have to be duplicated in each control set option. A "control set for right" ("CSR") 910 contain a similar list for control sets within a given right. "Control set 0" and any "control sets for rights" are thus, as mentioned above, optimizations; the same functionality fir the control set can be accomplished by listing all the common required methods in each control set option and omitting "control set 0" and any "controls set for rights." ('193 150:30) [see Fig. 26] - "Rights and permissions clearinghouses 400 may then distribute a new, combined control set 188ABC consistent with each of the individual control sets 188A, 188B, 188C—relieving he value chain participants form having to formulate any control sets other than the one they are particularly concerned about." ('712 190:14-18)

Claim Term	MS Construction
	- "May form an overall transaction control set from a number of discrete sub-control sets contributed, for example, by a number of different participants." ('712 234:12-15) "Transaction authority 700 also receives another control set 188X specifying how to link the various participants' control sets together into overall transactions processes with requirements and limitations (Figures 58A and 58B, block 752). The overall transaction control set 188Y specifies how to resolve conflicts between the sub-transaction control set 188 (1), 188 (N) provided by the individual participants (this could involve, for example, an electronic negotiation process 798 as shown in Figures 75A-76A of the Ginter et al. patent disclosure). The transaction authority 700 combines the participant's individual control sets – trying them together with additional logic create an overall transaction control superset 188Y (Figures 58A and 58B, block 752)." ('712 243:8-19) Extrinsic:
hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Intrinsic: - "Referring to FIG. 110, appliance 600 may then deliver the secure container(s) 302 to the intended recipient 4056 and/or to trusted electronic go-between 4700 based upon the instructions of sender 4052 as now reflected in the electronic controls 4078 associated with the object 300 (FIG. 110, block 4514). Such delivery is preferably by way of electronic network 4058 (672), but may be performed by any convenient electronic means such as, for example, Internet, Electronic Mail or Electronic Mail Attachment, WEB Page Direct, Telephone, floppy disks, bar codes in a fax transmission, filled ovals on a form delivered through physical mail, or any other electronic means to provide contact with the intended recipient(s)." ('683 40:10) - while grandparent ('107) did not refer to fax transmission or physical mail, it did recite that the delivery means could be by "physical storage media" or by transferring "physical things" ('193 3:28, 5:4, 14:21, 18:10, 53:33, 127:6, 245:32) - Those programs may communicate with the PPE 650 component of a user's electronic appliance 600 to make VDE-protected documents available for use while limiting the extent to which their contents may be copied, stored, viewed, modified, and/or transmitted and/or otherwise further distributed outside the specific electronic appliance. ('193 279:3) - Extrinsic:
'721:1	Intrinsic: USP 5,757,914 USP 4,930,703 "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2
digitally signing a first load module with a first digital signature designating the first load module for use by a first	Intrinsic: - "A hierarchy of assurance levels may be provided for different protected processing environment security levels. Load modules or other executables can be provided with digital signatures associated with particular assurance levels. Appliances assigned to particular assurance levels can protect themselves from executing load modules or other executables associated with different assurance levels. Different digital signatures and/or certificates may be used to distinguish between load modules or other executables intended for different assurance levels." ('721 6:16)

Claim Term	MS Construction
device class	- "Encryption can be used in combination with the assurance level scheme discussed above to ensure that load modules or other executables can be executed only in specific environments or types of environments. The secure way to ensure that a load module or other executable can't execute in a particular environment is to ensure that the environment doesn't have the key(s) necessary to decrypt it." ('721 6:63) - "A protected processing environment(s) of assurance level I protects itself (themselves) by executing only load modules 54 sealed with an assurance level I digital signature 106(I). Protected processing environment(s) 108 having an associated assurance level I is (are) securely issued a public key 124(I) that can "unlock" the level I digital signature. Similarly, a protected processing environment(s) of assurance level II protects itself (themselves) by executing only the same (or different) load module 54 sealed with a "Level II" digital signature 106(II). Such a protected processing environment 108 having an associated corresponding assurance level II possess a public key 124(II) used to "unlock" the level II digital signature. A protected processing environment(s) 108 of assurance level III protects itself (themselves) by executing only load modules 54 having a digital signature 106(III) for assurance level III. Such an assurance level III protected processing environment 108 possesses a corresponding assurance level 3 public key 124(III)." ('721 17:48) - "More specifically, a particular assurance level appliance 61 thus protects itself from using a load module 54 of a different assurance level. Digital signatures (and/or signature algorithms) 106 in this sense create the isolated "desert islands" shown--since they allow execution environments to protect themselves from "off island" load modules 54 of different assurance levels." ('721 19:61) "If a load module is encrypted differently for different assurance levels, and the keys and/or algorithms that are used to decrypt such load modules are only distributed to environments of the same assurance level, an additional measure of security is provided." ('721 20:7) Extrinsic:
digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class	Intrinsic: - "In one example, verifying authority 100 may digitally sign identical copies of load module 54 for use by different classes or "assurance levels" of electronic appliances 61." - "Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. Tamper resistant barriers may be used to protect this programming or other conditioning. The assurance levels described below are a measure or assessment of the effectiveness with which this programming or other conditioning is protected." - "For example, protected processing environments or other secure execution spaces that are more impervious to tampering (such as those providing a higher degree of physical security) may use an assurance level that isolates it from protected processing environments or other secure execution spaces that are relatively more susceptible to tampering (such as those constructed solely by software executing on a general purpose digital computer in a non-secure location)." ('721 6:34) - "The present invention may use a verifying authority and the digital signatures it provides to compartmentalize the different electronic appliances depending on their level of security (e.g., work factor or relative tamper resistance)." - "Assurance level I might be used for an electronic appliance(s) 61 whose protected processing environment 108 is based on software techniques that may be somewhat resistant to tampering. An example of an assurance level I electronic appliance 61A might be a general purpose personal computer that executes software to create protected processing environment 108. An assurance level II electronic appliance 61B may provide a protected processing environment 108 based on a hybrid of software security techniques and hardware-based security techniques. An example of an assurance level II electronic appliance 61B might be a general purpose personal computer equipped with a hardware

Claim Term	MS Construction
	integrated circuit secure processing unit ("SPU") that performs some secure processing outside of the SPU (see Ginter et al. patent disclosure FIG. 10 and associated text). Such a hybrid arrangement might be relatively more resistant to tampering than a software-only implementation. The assurance level III appliance 61C shown is a general purpose personal computer equipped with a hardware-based secure processing unit 132 providing and completely containing protected processing environment 108 (see Ginter et al. FIGS. 6 and 9 for example). A silicon-based special purpose integrated circuit security chip is relatively more tamper-resistant than implementations relying on software techniques for some or all of their tamper-resistance." "Assurance level in this example may be assigned to a particular protected processing environment 108 at initialization (e.g., at the factory in the case of hardware-based secure processing units). Assigning assurance level at initialization time facilitates the use of key management (e.g., secure key exchange protocols) to enforce isolation based on assurance level. For example, since establishment of assurance level is done at initialization time, rather than in the field in this example, the key exchange mechanism can be used to provide new keys (assuming an assurance level has been established correctly)." Extrinsic:
distributing the first load module for use by at least one device in the first device class	See above.
distributing the second load module for use by at least one device in the second device class	See above.
'721:34	Intrinsic: USP 5,757,914 USP 4,930,703 "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
arrangement within the first tamper resistant barrier	Intrinsic: An important part of VDE provided by the present invention is the core secure transaction control arrangement, herein called an SPU (or SPUs), that typically must be present in each user's computer, other electronic appliance, or network. ('193 48:66) Extrinsic:
prevents the first secure execution space from executing the same executable	Intrinsic: "In accordance with this feature of the invention, verifying authority 100 supports all of these various categories of digital signatures, and system 50 uses key management to distribute the appropriate verification keys to different assurance level devices. For example, verifying authority 100 may digitally sign a particular load module 54 such that only hardware-only based server(s) 402(3) at

Claim Term	MS Construction
accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level	assurance level XI may authenticate it. This compartmentalization prevents any load module executable on hardware-only servers 402(3) from executing on any other assurance level appliance (for example, software- only protected processing environment based support service 404(1))." ('721 19:11) Extrinsic:
'861:58	Intrinsic: "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
creating a first secure container	Intrinsic: - "For example, the descriptive data structure may be used in a creation process 302. The creation process 302 may read the descriptive data structure and, in response, create an output file 400 with a predefined format such as, for example, a container 100 corresponding to a format described by the descriptive data structure 200." ('861 11:58; Fig. 3) - "The output of the layout tool 300 may be a descriptive data structure 200 in the form of, for example, a text file. A secure packaging process 302a may accept container specific data as an input, and it may also accept the descriptive data structure 200 as a read only input. The packager 302a could be based on a graphical user interface and/or it could be automated. The packager 302a packages the container specific data 314 into a secure container 100. It may also package descriptive data structure 200 into the same container 100 if desired." ('861 12:9, and see Fig. 4) - "Descriptive data structure 200 may provide encodings of other characteristics in the form of metadata that can also be used by application 506 during a process of creating, using or manipulating container 100." ('861 13:30) - "This invention relates to techniques for defining, creating, and manipulating rights management data structures." ('861 1:23) - "Therefore, the container creation and usage tools must themselves be secure in the sense that they must protect certain details about the container design." ('861 4:59) - "The above-referenced Ginter et al. patent specification describes, by way of non-exhaustive example, "templates" that can act as a set (or collection of sets) of control instructions and/or data for object control software. See, for example, the "Object Creation and Initial Control Structures," "Templates and Classes," and "object definition file," "information" method and "content" methods discussions in the Ginter et al. specification. The described templates are, in at least some examples, capable of creating (and/or modifying) objects in a process that interacts with user instructions and provided content to create an object." ('861 4:65) - "The DDS creation tool 800 (see FIG. 10A) may then package the resulting DDS 200 into a secure container 100 along with an associated object 830" ('861 19:62) - "In accordance with one aspect of how to advantageously use descriptive data structures in accordance with a preferred embodiment of this invention, a machine readable descriptive data structure may be created by a provider to describe the layout of the provider's particular rights management data structure(s) such as secure containers. These descriptive data structure ("DDS") templates may be used to create containers." ('861 6:24) - "Object construction stage 1230 may use information in object configuration file 1240 to assemble or modify a container. This process typically involves communicating a series of events to SPE 503 to create one or more PERCs 808, public headers, private headers, and to encrypt content, all for storage in the new object 300 (or within secure database 610 within records associated with the new object)."

Claim Term	MS Construction
	('193 103:47) - "The Internet Repository 3406 VDE containerizes, including encrypts, selected object content as it streams out of the Repository in response to an online, user request to download an object." ('193 313:33) - "The container manager 764 may, in cooperation with SPE 503, construct an object container 302 based at least in part on parameters about new object content or other information as specified by object configuration file 1240. Container manager 764 may then insert into the container 302 the content or other information (as encrypted by SPE 503) to be included in the new object. Container manager 764 may also insert appropriate permissions, rules and/or control information into the container 302 (this permissions, rules and/or control information may be defined at least in part by user interaction through object submittal manager 774, and may be processed at least in part by SPE 503 to create secure data control structures). Container manager 764 may then write the new object to object repository 687, and the user or the electronic appliance may "register" the new object by including appropriate information within secure database 610. " ('193 104:12) [see Fig. 12A] Extrinsic:
including or addressing . . . organization information . . . desired organization of a content section. . . and metadata information at least in part specifying at least one step required or desired in creation of said first secure container	Intrinsic: - "metadata fields 264 (which may be part of and/or referenced by the descriptive data structure)" ('861 14:20); "include or reference" ('861 15:21); advantages of referencing ('861 15:32-58); alternative to referencing is "explicitly include" ('861 15:59); "including or addressing" (861.58); "includes a reference to" (861.69); - " it may be useful to store the metadata in a secure container 100 separately from DDS 200" ('861 15:35) - FIG. 7 shows an example of how descriptive data structure 200 may be formatted. As mentioned above, descriptive data structure 200 may comprise a list such as a linked list. Each list entry 260(1), 260(2), . . . may include a number of data fields including, for example: an object name field 262, one or more metadata fields 264 (which may be part of and/or referenced by the descriptive data structure); and location information 266 (which may be used to help identify the corresponding information within the container data structure 100)." - "a descriptive data structure could serve as `instructions` that drive an automated packaging application for digital content and/or an automated reader of digital content such as display priorities and organization (e.g., order and/or layout)."('861 7:54); - "a DDS 200 could serve as the `instructions` that drive an automated packaging application for digital content or an automated reader of digital content." ('861 13:) - "In accordance with one example, the machine readable descriptive data structure provides a description that reflects and/or defines corresponding structure(s) within the rights management data structure. For example, the descriptive data structure may provide a recursive, hierarchical list that reflects and/or defines a corresponding recursive, hierarchical structure within the rights management data structure. ... descriptive data structure may directly and/or indirectly specify where, in an associated rights management data structure, corresponding defined data types may be found." ('721 5:56); - Issued claim 1: a first memory storing a descriptive data structure, said descriptive data structure including: information regarding a first organization of elements within a secure container, said information including: information on the organization of said elements within said secure container; and information on the location of at least some of said elements within said secure container; " Issued claim 16: "using said organization information to identify a specific portion of said first secure container content." (see c. 17-19 re. specific specific portions) - Issued claim 34: "a representation of the format of data contained in a first rights management data structure said representation including: element information contained within said first rights management data structure; and organization information regarding the organization of said elements within said first rights management data structure; and information relating to metadata, said metadata including"

Claim Term	MS Construction
	- Issued claim 45 (dependent from 34-44): "said information regarding elements contained within said first rights management data structure includes information relating to the location of at least one such element." - Issued claim 73: "said descriptive data structure organization information includes information specifying that said first secure container contents will include at least a title and a text section referred to by said title." - Issued claim 74: "said descriptive data structure organization information includes information specifying that said first secure container contents will include at least one advertisement." - Issued claim 75: "said descriptive data structure further includes information relating to the location at which said title, said text section and said advertisement should be stored in said first secure container." - Issued claim 76: "at least a portion of said descriptive data structure organization information includes information specifying fields relating to at least one atomic transaction" - "For example, the FIG. 2A example descriptive data structure headline definition 202a does not specify a particular headline (e.g., "Yankees Win the Pennant!"), but instead defines the location (for example, the logical or other offset address) within the container data structure 100a (as well as certain other characteristics) in which such headline information may reside." ('861 10:54); "layout "hints" and field definitions (e.g., text, text block, integer, file, image or other data type)." ('861 16:49) - "A method of creating a first secure container, said method including the following steps;" ('861 this claim 58) "Descriptive data structure 200 can, for example, tell application 506 to always display a certain field (e.g., the author or copyright field) and to never display other information (e.g., information that should be hidden from most users)." ('861 13:) Extrinsic:
at least in part determine specific information required to be included in said first secure container contents	Intrinsic: - "Descriptive data structure 200 may provide encodings of other characteristics in the form of metadata that can also be used by application 506 during a process of *creating*, using or manipulating container 100. The DDS 200 can be used to generate a software program to manipulate rights management structures. For example, a DDS 200 could serve as the 'instructions' that drive an automated packaging application for digital content or an automated reader of digital content." ('861 13:30);. - "such metadata may impose integrity or other constraints during the creation and/or usage process (e.g., "when you create an object, you must provide this information", or "when you display the object, you must display this information")." ('861 15:25); "many possible integrity constraints.... Required: ... Optional ... Required relationship ... Optional relationship ... Repetition" ('861 16:15); - " "construction type" metadata (upon object construction, the information is required; upon object construction, the object creation tool is to always or never prompt for the information)" ('861 16:41); The descriptive data structure can be used to generate one or more portions of software programs that manipulate rights management structures. For example, a descriptive data structure could serve as 'instructions' that drive an automated packaging application for digital content and/or an automated reader of digital content such as display priorities and organization (e.g., order and/or layout)." ('861 7:51) "In use, electronic appliance 500 may access secure container 100 and--in accordance with rules 316--access the descriptive data structure 200 and content 102 it contains and provide it to application 506. The interpreter 508 within application 506 may, in turn, read and use the descriptive data structure 200." For example, suppose the application 506 wants to display the "headline" information within newspaper style content shown in FIG. 2A. Application 506 may ask interpreter 508 to provide it with information that will help it to locate, read, format and/or display this "headline" information." ('861 12:57)

Claim Term	MS Construction
	Extrinsic:
rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents	Intrinsic: Prosecution History of '861 Patent: "Claims [1,10,25,26] are rejected under 35 U.S.C. 102(b) as being clearly anticipated by the common and decades-old practice of using database schema to describe the structure of a database which requires password/identifications for access. ... Claims [1-17,25-26] are rejected under 35 U.S.C. 102(a) as being anticipated by Anderson et al (Anderson), USP 5,537,526, Method and Apparatus for Processing a Display Document Utilizing a System Level Document. The claims are rejected on the basis of the correspondence between the teachings of Anderson and the elements of the claims as follows: As to claim 1 (and 10), the TabstractModel 502 is a machine readable, abstract descriptive data structure which interoperates with Tmodels 506 (TM), and TmodelSurrogates 504 (TMS). ... These models are clearly data structures, and while they can be of many types, the data they manage can include restrictions that correspond to rights management." 08/805,804 ('861), Office Action, 06/25/98, p. 2-3 - "The rights management environment in which DigiBox.TM. containers are used allows commerce participants to associate rules with the digital information (content)." ('861 1:50) - "For example, a creator of content can package one or more pieces of digital information with a set of rules in a DigiBox secure container--such rules may be variably located in one or more containers and/or client control nodes--and send the container to a distributor. The distributor can add to and/or modify the rules in the container within the parameters allowed by the creator. The distributor can then distribute the container by any rule allowed (or not prohibited) means--for example, by communicating it over an electronic network such as the Internet. A consumer can download the container, and use the content according to the rules within the container. The container is opened and the rules enforced on the local computer or other InterTrust-aware appliance by software InterTrust calls an InterTrust Commerce Node. The consumer can forward the container (or a copy of it) to other consumers, who can (if the rules allow) use the content according to the same, differing, or other included rules--which rules apply being determined by user available rights, such as the users specific identification, including any class membership(s) (e.g., an automobile club or employment by a certain university). In accordance with such rules, usage and/or payment information can be collected by the node and sent to one or more clearinghouses for payment settlement and to convey usage information to those with rights to receive it." ('861 2:13) - "Descriptive data structure 200 may supply integrity constraints or rules that protect the integrity of corresponding content during use of and/or access to the content." ('861 12:2) - "For example, DDS 200 can specify that an article of a newspaper cannot be viewed without its headline being viewed. The corresponding integrity constraint can indicate the rule 'if there is an article, there must also be a headline'." ('861 16:2) "In this example, each target data block 801 includes rule (control) information. Different target data blocks 801 can provide different rule information for different target environments 850. The rule information may, for example, relate to operations (events) and/or consequences of application program functions 856 within the associated target environment 850 such as specifying:" ('861 18:33) Extrinsic:
'891:1	Intrinsic: "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2

Claim Term	MS Construction
	See "Virtual Distribution Environment" above.
resource processed in a secure operating environment at a first appliance	Intrinsic: - Prosecution History of Application 08/388,107 (issued at '891): "Please amend the remaining claims as follows: 15. (Amended) A method for [managing] using at least one resource [with] processed in a secure operating environment at a first appliance, said method comprising: securely receiving a first entity's control [from a first entity] at said first appliance, said first entity being located remotely from [external to] said operating environment and said first appliance; securely receiving a second entity's control [from a second entity] at said first appliance, said second entity being located remotely from [external to] said operating environment and said first appliance, said second entity being different from said first entity; and securely processing a data item at said first appliance, using at least one resource [, a data item associated with said first and second controls; and], including securely applying, at said first appliance through use of said at least one resource, said first entity's control and said second entity's control [controls] to [manage said resource for] govern use [with] of said data item." 08/388,107, Amendment, 06/20/97, p. 2 (MSI028825) Extrinsic:
securely receiving a first entity's control at said first appliance	See above.
securely receiving a second entity's control at said first appliance	See above.
securely processing a data item at said first appliance, using at least one resource	Intrinsic: "a protected processing environment, coupled to said communications arrangements, that: (a) securely processing, using at least one resource, a data item associated with said first and second controls, and (b) securely applies said first and second controls to manage said resources for use of said data item." (08/388,107 page 781 claim 75) Extrinsic:
securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item	Intrinsic: "Such secure combination of VDE manage pieces of content will frequently require VDE's ability to securely derive content control information which accommodates the control information requirements, including any combinational rules, of the respective VDE managed pieces of content and reflects an acceptable agreement between plural control information sets." (293:12 Extrinsic:
'900:155	Intrinsic: "The instant application is one of a series of applications which are all generally directed to a virtual

Claim Term	MS Construction
	distribution environment."

09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2

Prosecution History of '900:

Claims 302, 321 and 322, as pending:
"302. A virtual distribution environment comprising
- a first host processing environment comprising
- a central processing unit;
- main memory operatively connected to said central processing unit;
- mass storage operatively connected to said central processing unit and said main memory;
- said mass storage storing tamper resistant software designed to be loaded into said main memory and executed by said central processing unit, said tamper resistant software comprising:
- machine check programming which derives information from one or more aspects of said host processing environment,
- one or more storage locations storing said information; and
- integrity programming which
- causes said machine check programming to derive said information,
- compares said information to information previously stored in said one or more storage locations, and
- generates an indication based on the result of said comparison.
321. A virtual distribution environment as in claim 302,
- said virtual distribution environment further comprising programming which takes one or more actions based on the state of said indication.
322. A virtual distribution environment as in claim 321 in which said one or more actions includes at least temporarily halting further processing."
(08/706,206 ('900), Amendment, 06/09/98, 92-93, 96, 96-97)

"Claims ... 322-324, ... are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims."
08/706,206 ('900), Office Action, 08/27/98, p. 2

"322. A virtual distribution environment comprising
- a first host processing environment comprising
- a central processing unit;
- main memory operatively connected to said central processing unit;
- mass storage operatively connected to said central processing unit and said main memory;
- said mass storage storing tamper resistant software designed to be loaded into said main memory and executed by said central processing unit, said tamper resistant software comprising:
- machine check programming which derives information from one or more aspects of said host processing environment,
- one or more storage locations storing said information;
- integrity programming which
  - causes said machine check programming to derive said information,
  - compares said information to information previously stored in said one or more storage locations, and
  - generates an indication based on the result of said comparison; and
- programming which takes one or more actions based on the state of said indication;
- said one or more actions including at least temporarily halting further processing."
(pg. 27-28)
Remarks, "Applicants appreciate the indication that claims ... are allowed and that claims ... 322-324

Claim Term	MS Construction
	are objected to but would be allowable if rewritten into independent form. ... For purposes of expedition, applicants are cancelling the rejected claims without prejudice ..., and are rewriting objected to dependent claims into independent form." (pg. 42) 08/706,206 ('900), Amendment, 11/23/98, p. 27-28, 42
first host processing environment comprising	See above.
said mass storage storing tamper resistant software	See above.
designed to be loaded into said main memory and executed by said central processing unit	See above.
said tamper resistant software comprising: ... one or more storage locations storing said information	Intrinsic: "Referring once again to FIG. 69B, the installed operational materials 3472 may be further customized for each instance by making random changes to reserved, unused portions of the operational materials (FIG. 69B, block 3470(6)). An example of this is shown in FIG. 69E. In this example, the operational materials 3472 include unused, embedded random data or code portions 3494." Extrinsic:
derives information from one or more aspects of said host processing environment,	Intrinsic: ('900 73:1 - 80: 6); ('900 230:55 - 233:34); ('900 235:28-244:15); Figs. 69A-N
one or more storage locations storing said information	Intrinsic: "Referring once again to FIG. 69B, the installed operational materials 3472 may be further customized for each instance by making random changes to reserved, unused portions of the operational materials (FIG. 69B, block 3470(6)). An example of this is shown in FIG. 69E. In this example, the operational materials 3472 include unused, embedded random data or code portions 3494."
information previously stored in said one or more storage locations	Intrinsic: See terms.
generates an indication based on the result of said comparison	See terms.
programming which takes one or more actions based on the state of said indication	Intrinsic: Claim 321, as pending: "321. A virtual distribution environment as in claim 302, said virtual distribution environment further comprising programming which takes one or more actions

Claim Term	MS Construction
	based on the state of said indication." 08/706,206 ('900), Amendment, 06/09/98, p. 96
at least temporarily halting further processing	See halting.
'912:8	"The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
identifying at least one aspect of an execution space required for use and/or execution of the load module	Intrinsic: "For each site, the manufacturer generates a site ID 2821 and list of site characteristics 2822." ('193 209:55)
said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security	Extrinsic: See generally processor identification field, memory maps, and address spaces. (Tanenbaum, A., Modern Operating Systems, MS1096004)
checking said record for validity prior to performing said executing step	Extrinsic: Validity Check: The process of analyzing data to determine whether it conforms to predetermined completeness and consistency parameters. (Microsoft Computer Dictionary, 3rd ed. 1997)

Claim Term	MS Construction
'912:35	"The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
received in a secure container	See terms.
said component assembly allowing access to or use of specified information	See terms.
said first component assembly specified by said first record	See terms.

Exhibit E

Exhibit E

Microsoft's Statement of Reservations

Microsoft provides its attached claim construction for each of the 12 "Mini-Markman" claims, subject to the limitations and reservations of rights set forth herein.

Claim Invalidity: Microsoft does not waive any defenses that the asserted claims fail to satisfy the provisions of 35 U.S.C. § 112, including, for example, the written description requirement, the definiteness requirement, or any other requirement for patentability. Microsoft does not concede that the asserted claims are supported by Plaintiff's original "big book" application or any application from which they purportedly claim priority. By offering a construction of a term, Microsoft does not waive any defense that the claim is indefinite and there can be no proper construction.

Continuing Discovery: Microsoft reserves the right to modify its claim constructions in light of ongoing claim construction discovery. Microsoft reserves the right to modify or supplement its cited extrinsic evidence in light of information which is provided in continuing claim construction discovery, or information which has already been provided but too recently, or in too high a volume, or in other manner inhibiting its full review, such as InterTrust's re-production of over 1,000,000 pages on November 4, 2002.

Intrinsic Evidence: For the purposes of submission of this claim construction only, Microsoft treats the "intrinsic" evidence as including: 1) the specifications of each of the seven U.S. patents at issue in the "Mini-Markman" proceeding, including any material purportedly incorporated by reference therein; 2) the prosecution history of each of the seven patents at issue, including the applications and prosecution history of the seven patents and any related patent applications, including without limitation, applications purportedly incorporated by reference or to which an application claimed priority; and 3) all references cited in the prosecution of any such applications.

Microsoft does so without waiving the right to contest whether some of this information is or is not properly part of the intrinsic evidence.

Exhibit F

Exhibit F

Dr. Reiter is expected to testify as follows:

1. Dr. Reiter will testify regarding the meaning of the disputed claim elements to one of ordinary skill in the art, taking into account the understood meaning of the terms in the art, the patent specifications and the file histories. He will testify as follows:

a. InterTrust's proposed definitions, attached as Exhibit B to the Joint Claim Construction Statement ("JCCS") are consistent with the use of the terms or phrases in the specification and the relevant art. Those definitions are attached hereto. Citations to supporting specification text and relevant art can be found in Exhibit C to the JCCS.

b. Microsoft has made repeated substantial changes to its proposed definitions, the changes continuing up to shortly before the present document was prepared. For this reason, it is impossible to include detailed responses to the issues raised by those definitions.

In general, however, the Microsoft definitions incorporate restrictions that are inconsistent with specification use of the terms and/or inconsistent with the understanding of the terms in the art. Those inconsistencies are demonstrated by the attached supporting evidence. The following discussion lists one or more serious deficiencies in each Microsoft definition, but is not intended as a comprehensive description of all such deficiencies.

Individual terms

Access/Access to/Accessing/Accessed

The first sentence of Microsoft's definition is generally consistent with the InterTrust definition. The second sentence of the Microsoft definition is based on a specific disclosed embodiment, and is inconsistent with general use of the term in the specifications.

Addressing

The two parties' definitions are very close. Microsoft's definition is, however, improper in its apparent exclusion of indirect addressing.

Allowing, allows

Microsoft's definition is based on a specific disclosed embodiment and ignores other embodiments. See InterTrust's supporting evidence.

Arrangement

Microsoft's definition requires particular types of organizations and is therefore inconsistent with the patent specifications.

Aspect

Microsoft's definition is overly restrictive in its requirement that an aspect be "persistent" and that it "can be used to distinguish [an environment] from other environments."

Associated with

Microsoft's definition incorporates restrictions based on a particular embodiment and is inconsistent with other disclosed embodiments and with the general meaning of the term.

Authentication

Microsoft's definition requires multiple types of authentication, in a manner not required by use of this term in the specification or the art. Moreover, some of these types cannot be applied (e.g., "origin integrity" applied to an organization).

Authorization information, Authorized, Not authorized

Microsoft's definitions are based on specific embodiments and contradicted by alternative embodiments disclosed in the specifications.

Budget control; Budget

Microsoft's definition improperly restricts "budget" to a particular type of method, and improperly restricts Budget Control in a manner inconsistent with the specification.

Can be

Microsoft's definition incorporates the language "which otherwise cannot be carried out." This language is inconsistent with the specifications.

Capacity

The Microsoft definition relates to hardware storage devices, a context that is irrelevant to use of the term in the relevant claim.

Clearinghouse

Microsoft's definition is inconsistent with use of this term in the specifications. See InterTrust's supporting evidence.

Compares; Comparison

Microsoft's definition is based on a particular type of processor operation, a context that is not discussed in the specification and not required by the claim.

Component assembly

Microsoft's definition incorporates a large number of restrictions based on specific embodiments and ignoring alternate embodiments.

Contain, contained, containing

Microsoft's definition requires "physically" or "directly" storing, and distinguishes Addressing. This is inconsistent with use of the term in the specification.

Control (n.); Controls (n.)

The Microsoft definition incorporates a large number of restrictions based on specific embodiments, and ignores alternate embodiments described in the specifications.

Controlling; Control (v.)

The Microsoft definition incorporates limitations that are not required by the specification, including limitations contradicted by use of the term in the specifications and by disclosed embodiments.

Copied file

The Microsoft definition improperly distinguishes "copied file" from "copy."

Copy, copied, copying (v.)

The Microsoft definition is internally inconsistent, since it both prohibits and allows changes in the reproduced file. That definition also incorporates examples that are inconsistent with use of the terms in the claims.

Copy control

The Microsoft definition is inconsistent with use of this term in the claim.

Data item

The Microsoft definition incorporates limitations not present in the InterTrust definition. These limitations are not required by the specification or normal use of the term in the art.

Derive, Derives

The Microsoft definition requires retrieval, a concept not required by the specifications or use of this term in the claim.

Descriptive data structure

Limitations in the last two sentences of the Microsoft definition are inconsistent with described embodiments and are not required by the specifications or use of the term in the claims.

Designating

The Microsoft definition does not apply to this term, but instead to the claim phrase in which the term is found. That claim phrase is separately defined.

Device class

The Microsoft definition is inconsistent with the definition given to this term during prosecution.

Digital file

The Microsoft definition is overly restrictive. The limitations is incorporates are not required by the specification, use of the term in the claims or general use in the relevant art.

Digital signature; Digitally signing

The Microsoft definition of digital signature requires that the string be "computationally unforgeable," a characteristic that is impossible to obtain. The Microsoft definition of digitally signing requires a secret key, and also includes significant background discussion not necessary for the definition.

Entity's control

Microsoft's definition improperly requires control of a "particular use of or access to particular protected information by a particular user(s)." No such requirements are imposed by the term, the claim or the specifications.

Environment

Microsoft does not appear to have provided any definition for this term.

Executable programming; Executable

Microsoft's requirement of "machine code instructions" is inconsistent with use of this term in the specifications. In addition, Microsoft's definition of "computer program" imposes limitations not required by these terms.

Execution space; Execution space identifier

Microsoft's definition of Execution Space is inconsistent with the explicit definition given to this term during prosecution. Microsoft's definition of Execution Space Identifier improperly requires "unique" identification.

Governed item

Microsoft's definition of Governed Item requires arbitrarily fine granularity and control of "access and use by any user, process, or device." Neither the term nor the specifications require such limitations.

Halting

The Microsoft definition requires execution be "unconditionally" stopped. The specification imposes no such requirement, and the Microsoft definition appears to be based on a particular type of instruction that is not mentioned in the patents.

Host processing environment

The Microsoft definition incorporates the term "VDE node," a term that is itself defined at great length, incorporating numerous improper limitations. The Microsoft definition also improperly incorporates restrictions based on privileged mode versus user mode, and "loaded" software. In addition, the Microsoft definition improperly excludes hardware.

Identifier, Identify, Identifying

The Microsoft definitions improperly restrict these terms to "particular instances."

Including

The definitions are consistent, except that the hardware portion of Microsoft's definition requires "physically present within." This is inconsistent with use of the term in the claims.

Information previously stored

Microsoft's definition would render the claim nonsensical, since it would require a comparison involving information that is no longer available for the comparison.

Integrity programming

The Microsoft definition is internally inconsistent, improperly incorporates the term Executable Programming and improperly defines integrity as excluding all alterations.

Key

Microsoft's exclusion of "key seed or other information from which the actual encryption and/or decryption key is constructed, derived, or otherwise identified" is inconsistent with the specification and general use of the term in the relevant art.

Load module

Microsoft's definition imposes numerous limitations beyond those identified in the InterTrust definition. Those additional limitations are not required by the term and are inconsistent with embodiments disclosed in the specifications.

Machine check programming

The Microsoft definition improperly requires Executable Programming and a "unique 'machine signature' which distinguishes the physical machine from all other machines." These limitations are not required by the term.

Opening secure containers

The Microsoft definition improperly distinguishes "opening" from decrypting, and improperly incorporates limitations based on a particular embodiment of opening.

Operating environment

See Processing Environment.

Organization, Organization information, Organize

The Microsoft definitions improperly incorporate concepts related to physical storage.

Portion

The Microsoft definition improperly implies that presence of a "portion" excludes presence of the whole.

Prevents

The Microsoft definition requires a level of certainty that is inconsistent with the specification and impossible to obtain.

Processing Environment

The Microsoft definition incorporates a specific embodiment and would exclude other embodiments disclosed for this term.

Protected processing environment

The Microsoft definition incorporates at least several dozen highly restrictive and unnecessary limitations, and appears to combine restrictions from multiple separate embodiments.

Protecting

The incorporation of Security into the Microsoft definition is improper, since that term is considerably more general than the manner in which Protecting is used in the claim.

Record

The Microsoft definition includes limitations beyond those incorporated in the InterTrust definition. These added limitations are not required by use of this term in the claims, specification, or art.

Required

The Microsoft definition implies a degree of absoluteness that is inconsistent with the specification. The second sentence of the Microsoft definition is unsupported by the specification or normal use of the term.

Resource processed

The Microsoft definition improperly requires a "shared facility," and that the resource be "required by a job or task." These are not required by the claim or specification.

Rule

The Microsoft definition improperly distinguishes Rules from Controls, and imposes an unsupported requirement that a Rule be a "lexical statement."

Secure

The Microsoft definition requires absolute protection against all possible threats, and is therefore inconsistent with use of the term in the specification, the claims, and the relevant art.

Secure container

The requirements imposed by the Microsoft definition are either inconsistent with the specification or ignore disclosed embodiments.

Secure container governed item

The Microsoft definition imposes a requirement of absolute security that is inconsistent with the specification and ignores alternate disclosed embodiments.

Secure database

The Microsoft definition improperly defines "database" in accordance with one particular type of database, and improperly imposes a requirement of absolute security that is inconsistent with the specification.

Secure execution space

The Microsoft definition is inconsistent with and excludes embodiments of Secure Execution Spaces described in the specification.

Secure memory

Microsoft's definition of "memory" improperly excludes virtual memory. Microsoft's definition of Secure Memory includes numerous restrictions not supported by the specification.

Secure operating environment, Said operating environment

See Secure Processing Environment.

Securely applying

Microsoft's definition of "securely" is inconsistent with and excludes embodiments described in the specification.

Microsoft's definition of Securely Applying improperly includes limitations from specific embodiments, as well as limitations not required by the specification or claims.

Securely assembling

The Microsoft definition incorporates limitations from specific embodiments, and ignores alternate embodiments not requiring those limitations.

Securely processing

The Microsoft definition improperly incorporates a requirement of a secure execution space. This requirement is inconsistent with embodiments described in the specification.

Securely receiving

The Microsoft definition is based on limitations taken from a particular embodiment and ignores alternate embodiments.

Security level, Level of security

The Microsoft definition improperly requires an "ordered measure" and persistence. The second and third sentences from the Microsoft definition are unsupported by any disclosure in the specifications.

Tamper resistance

The Microsoft definition improperly requires a tamper resistant barrier.

Tamper resistant barrier

The Microsoft definition describes a specific embodiment, and is inconsistent with alternate embodiments described in the specifications.

Tamper resistant software

The Microsoft definition improperly requires a tamper resistant barrier.

Use

The second sentence of the Microsoft definition improperly incorporates limitations from a particular embodiment.

User controls

The Microsoft definition is inconsistent with the claim and the prosecution history.

Validity

The Microsoft definition improperly incorporates the concept of "authentication," and applies only to data.

Virtual distribution environment

See Global Construction of VDE.

Claim phrases

193.1

receiving a digital file including music

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication a recipient and use of controls.

a budget specifying the number of copies which can be made of said digital file

The Microsoft definition improperly includes "copies" that are not "long-lived, decrypted or accessible." The Microsoft definition also ignores embodiments involving alternative control structures.

controlling the copies made of said digital file

The Microsoft definition improperly incorporates limitations from particular embodiments, ignores embodiments describing alternative control structures and imposes numerous limitations that are not supported by the specification or claim language.

determining whether said digital file may be copied and stored on a second device based on at least said copy control

The Microsoft definition incorporates numerous unnecessary limitations not required by the claim or the specification, improperly requires that "the" file, as opposed to a copy, be stored on a second device, excludes described alternative embodiments and requires an absolute degree of control that is inconsistent with the specification.

if said copy control allows at least a portion of said digital file to be copied and stored on a second device

The Microsoft definition's "explanation" of the branches makes no sense and is unsupported by the claim and, improperly requires that "the" file, as opposed to a copy, be stored on a second device.

copying at least a portion of said digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly excludes embodiments described in the specification.

transferring at least a portion of said digital file to a second device

The Microsoft definition improperly distinguishes a "copy" and "the" file, improperly requires that controls be executed and ignores alternative embodiments described in the specification.

storing said digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly requires storage of the entire file rather than a portion.

193.11

receiving a digital file

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication a recipient and use of controls.

determining whether said digital file may be copied and stored on a second device based on said first control

The Microsoft definition incorporates numerous unnecessary limitations not required by the claim or the specification, improperly requires that "the" file, as opposed to a copy, be stored on a second device, excludes described alternative embodiments and requires an absolute degree of control that is inconsistent with the specification.

identifying said second device

The Microsoft definition improperly requires that the identification distinguish the device from all other devices, that controls be used and that a VDE Secure Processing Environment be used.

whether said first control allows transfer of said copied file to said second device

The Microsoft definition improperly distinguishes a "copy" from "the" file, and ignores embodiments describing alternative control structures.

said determination based at least in part on the features present at the device

The Microsoft definition improperly requires that all features be used, that these be "actual, current" features and improperly excludes device identifiers.

if said first control allows at least a portion of said digital file to be copied and stored on a second device

The Microsoft definition's "explanation" of the branches makes no sense and is unsupported by the claim and , improperly requires that "the" file, as opposed to a copy, be stored on a second device.

copying at least a portion of said digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly excludes embodiments described in the specification.

transferring at least a portion of said digital file to a second device

The Microsoft definition improperly distinguishes a "copy" and "the" file, improperly requires that controls be executed and ignores alternative embodiments described in the specification.

storing said digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly requires storage of the entire file rather than a portion.

193.15

receiving a digital file

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication a recipient and use of controls, and the requirement that the step must proceed in both authentication branches is not supported in the claim.

an authentication step comprising:

The Microsoft definition improperly includes a requirement of an absence of trust, VDE controls and a VDE Secure Processing Environment.

accessing at least one identifier associated with a first device or with a user of said first device

The Microsoft definition improperly requires "securely" accessing, that an identifier identify a "single" user or device (but not "and"), VDE controls, and a VDE Secure Processing Environment.

determining whether said identifier is associated with a device and/or user authorized to store said digital file

The Microsoft definition improperly requires VDE controls and a VDE Secure Processing Environment.

storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized

The Microsoft definition ignores embodiments describing alternative control structures, and improperly requires that "the" file be stored, as opposed to a copy, VDE controls, and a VDE Secure Processing Environment.

storing information associated with said digital file in a secure database stored on said first device, said information including at least one control

Microsoft's definition improperly requires that the stored information be associated with the digital file but not the digital file's contents, VDE controls, a VDE Secure Processing Environment and that the step proceed regardless of the outcome of the authentication step.

determining whether said digital file may be copied and stored on a second device based on said at least one control

The Microsoft definition incorporates numerous unnecessary limitations not required by the claim or the specification, improperly requires that "the" file, as opposed to a copy, be stored on a second device, excludes described alternative embodiments, requires an absolute degree of control that is inconsistent with the specification, and requires that the step proceed regardless of the outcome of the authentication step.

if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,

The Microsoft definition's "explanation" of the branches makes no sense and is unsupported by the claim and , improperly requires that "the" file, as opposed to a copy, be stored on a second device.

copying at least a portion of said digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly excludes embodiments described in the specification and improperly requires that the step proceed regardless of the outcome of the authentication step.

transferring at least a portion of said digital file to a second device

The Microsoft definition improperly distinguishes a "copy" and "the" file, improperly requires that controls be executed and ignores alternative embodiments

described in the specification, and improperly requires that the step proceed regardless of the outcome of the authentication step.

storing said digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly requires storage of the entire file rather than a portion, and improperly requires that the step proceed regardless of the outcome of the authentication step.

193.19

receiving a digital file at a first device

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication a recipient and use of controls.

establishing communication between said first device and a clearinghouse located at a location remote from said first device

The Microsoft definition improperly requires a communications channel and that the communications channel was "previously non-existent."

using said authorization information to gain access to or make at least one use of said first digital file

The Microsoft definition improperly requires that "all of" the authorization information be used, VDE controls, a VDE Secure Processing Environment, and ignores embodiments describing alternative control structures.

receiving a first control from said clearinghouse at said first device

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication a recipient and use of controls.

storing said first digital file in a memory of said first device

The Microsoft definition improperly requires VDE controls and a VDE Secure Processing Environment.

using said first control to determine whether said first digital file may be copied and stored on a second device

The Microsoft definition incorporates numerous unnecessary limitations not required by the claim or the specification, improperly requires that "the" file, as opposed

to a copy, be stored on a second device, excludes described alternative embodiments and requires an absolute degree of control that is inconsistent with the specification.

if said first control allows at least a portion of said first digital file to be copied and stored on a second device

The Microsoft definition's "explanation" of the branches makes no sense and is unsupported by the claim and , improperly requires that "the" file, as opposed to a copy, be stored on a second device.

copying at least a portion of said first digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly excludes embodiments described in the specification.

transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output

The Microsoft definition improperly distinguishes a "copy" and "the" file, improperly requires that controls be executed and ignores alternative embodiments described in the specification.

storing said first digital file portion

Microsoft's definition improperly distinguishes a "copy" and "the" file.

683.2

the first secure container having been received from a second apparatus

Microsoft's definition improperly requires that the first secure container identify the apparatus from which it was received, and improperly argues that, in the absence of such identification, that container could not be distinguished from a container created at the site. Microsoft's definition includes numerous improper limitations, including authenticating a recipient and authentication occurring in accordance with VDE controls. The examples cited by Microsoft are misleading, since these are specific embodiments rather than general requirements.

an aspect of access to or use of

Microsoft's definition improperly excludes rules governing more than one aspect, improperly excludes access and use and improperly requires that the aspect be governed in relation to "any and all processes, users, and devices."

the first secure container rule having been received from a third apparatus different from said second apparatus

Microsoft's definition improperly requires that the first secure container identify the apparatus from which it was received, and improperly argues that, in the absence of such identification, that container could not be distinguished from a container created at the site. Microsoft's definition includes numerous improper limitations, including receipt in a secure container, authenticating a recipient and authentication occurring in accordance with VDE controls.

hardware or software used for receiving and opening secure containers

Microsoft's definition improperly requires a Secure Processing Environment and SPU, improperly requires "the same single logical piece of either hardware or software (as opposed to both), " and improperly requires authentication and VDE controls.

said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers

The Microsoft definition improperly requires that rules be associated with secure containers, as opposed to governed items.

protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus

The Microsoft definition is unsupported in the specification. It is contradicted by the claim and improperly requires numerous elements not required by the specification, including a Secure Processing Environment.

hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container

The Microsoft definition improperly requires a Secure Processing Environment/SPU, a "single" piece of hardware or software, assembly of a control and governance through VDE controls.

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.

The Microsoft definition improperly requires a Secure Processing Environment/SPU, a "single" piece of hardware or software, assembly of a control and governance through VDE controls. The examples cited by Microsoft are misleading, since these are specific embodiments rather than general requirements.

721.1

digitally signing a first load module with a first digital signature designating the first load module for use by a first device class

The Microsoft definition improperly requires that the digital signature be used as the signature key, that all load modules be signed and that certain devices not have keys.

digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class

The Microsoft definition improperly requires that the digital signature be used as the signature key, that all load modules be signed, that certain devices not have keys, that security levels be persistent and that security levels be greater or less than other security levels.

distributing the first load module for use by at least one device in the first device class

The Microsoft definition improperly requires transmission and that the digital signature accompany the first load module as distributed.

distributing the second load module for use by at least one device in the second device class

The Microsoft definition improperly requires transmission and that the digital signature accompany the first load module as distributed.

721.34

arrangement within the first tamper resistant barrier

The Microsoft definition improperly requires that the arrangement be "executed wholly within the first tamper resistant barrier."

prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level

The Microsoft definition improperly requires that the second secure execution space be part of the protected processing environment, that security level differences be persistent and higher or lower than each other and that the "same" executable be executed.

861.58

creating a first secure container

The Microsoft definition improperly requires a VDE Secure Processing Environment.

including or addressing ... organization information ... desired organization of a content section. .. and metadata information at least in part specifying at least one step required or desired in creation of said first secure container

The second paragraph from Microsoft's definition is inconsistent with the claim. The limitations imposed by the third paragraph are not required by the claim or specification.

at least in part determine specific information required to be included in said first secure container contents

The Microsoft definition improperly excludes other reasons for inclusion of the information and improperly requires specific values.

rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents

The Microsoft definition improperly requires that the rule be designed for particular contents, that the rule be used by VDE controls, the presence of a VDE Secure Processing Environment and that the rule is generated or identified based on the descriptive data structure. Microsoft's definition also excludes embodiments describing alternative control structures.

891.1

resource processed in a secure operating environment at a first appliance

The Microsoft definition improperly requires a shared facility and a Secure Processing Unit with specific features.

securely receiving a first entity's control at said first appliance

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication, use of controls and encryption on the communications level.

securely receiving a second entity's control at said first appliance

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication, use of controls and encryption on the communications level.

securely processing a data item at said first appliance, using at least one resource

The Microsoft definition improperly requires a Secure Processing Unit including numerous limitations.

securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item

The Microsoft definition improperly requires a Secure Processing Environment consisting of a Secure Processing Unit and that the resource be a component part of a secure operating environment.

900.155

first host processing environment comprising

The Microsoft definition incorporates limitations not required by the claim or the specifications, including limiting the host processing environment to only currently executing software.

designed to be loaded into said main memory and executed by said central processing unit

The Microsoft definition improperly requires that the software is capable of being loaded "only" in the main memory and executed "only" by the CPU.

said tamper resistant software comprising: . . . one or more storage locations storing said information

The Microsoft definition improperly requires that the storage locations be part of the machine check programming and that the storage locations must not store other information.

derives information from one or more aspects of said host processing environment,

The Microsoft definition improperly requires that information be derived from "hardware," and that the information "uniquely and persistently" identify the host processing environment.

one or more storage locations storing said information

The Microsoft definition improperly requires that the storage locations be part of the tamper resistant software and that the storage locations must not store other information.

information previously stored in said one or more storage locations

Microsoft's definition would render the claim nonsensical, since it would require a comparison involving information that is no longer available for the comparison.

generates an indication based on the result of said comparison

Microsoft's definition improperly requires that only two results be possible and that the indication is based solely on the result of the "compares" step.

programming which takes one or more actions based on the state of said indication

The Microsoft definition improperly requires executable programming, that the programming not be part of the host processing environment, that the programming must take an action regardless of the indicator state and that the action must be based solely on the state of the indication.

at least temporarily halting further processing

Microsoft's definition improperly requires that the host processing environment and all processes running in it be halted.

912.8

identifying at least one aspect of an execution space required for use and/or execution of the load module

The Microsoft definition improperly requires that the identifier "define fully, without reference to any other information."

said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security

The Microsoft definition improperly requires that the execution space identifier provides the load module with the ability to determine a level of security, and the presence of two higher and two lower levels of security.

checking said record for validity prior to performing said executing step

The Microsoft definition improperly requires that the record be checked before execution of any identified information, that evaluation occur within a VDE Secure Processing Environment, and that specific types of information be checked.

912.35

received in a secure container

The Microsoft definition improperly requires "encapsulation" in a secure container, authentication in accordance with VDE controls and acceptance of the secured container.

said component assembly allowing access to or use of specified information

The Microsoft definition improperly requires that the component assembly operate by itself, that it execute in a VDE Secure Processing Environment and that the component assembly be dedicated to specific information. The Microsoft definition ignores embodiments describing alternative control structures and improperly distinguishes access and use.

said first component assembly specified by said first record

The first paragraph of Microsoft's definition defines this term in a restrictive manner with no support in the claim. Microsoft's second paragraph is devoted to a non-existent inconsistency created by Microsoft's restrictive definition.

Claims as a Whole:

In every case, Microsoft requires the system be a VDE or the method be performed in a VDE. This requirement is not supported by the language of any of the claims.

Global Construction

The language of the individual claims contains nothing to support the large number of restrictions imposed by Microsoft's "global construction." Those restrictions are unsupported by and in many cases contradicted by the specification.

2. Digital Rights Management in general. Dr. Reiter will testify regarding Digital Rights Management technology, including encryption and tamper-resistance techniques. The nature and extent of such testimony will depend on the Court's decision as to the scope and format of tutorial presentations.

3. InterTrust's patents and patent claims. Dr. Reiter will testify regarding the general nature of the InterTrust patents, and will summarize the claims at issue in the initial Joint Claim Construction hearing. The nature of that testimony will depend on the

Court's decision as to ordering and format of testimony, but will be consistent with the testimony outlined above regarding claim terms and phrases.

Exhibit G

Exhibit G

Summary of Opinions of Professor John Mitchell
In Support of Microsoft's Proposed Claim Constructions

1.   In the field of computer security, terms such as "secure," "protect," and "tamper resistance" are understood differently depending on the particular context in which they are used. They have such a range of possible meanings that context is essential to understanding what these terms mean in a given instance. The same is true for terms like "govern" and "control" when they are used to describe computer systems or access to information.

A person skilled in the computer security field would not expect to use a dictionary to understand what these terms mean in a given context; rather, he or she would expect to review the particular reference or system in question to see what adversarial events or attacks are being defended against. Generally speaking, dictionary "definitions" are not sufficient for understanding how these terms are meant in a particular case. A number of terms and phrases used in the February 1995 application (such as "VDE," "PPE," and "secure container") are also not likely to be found in dictionaries.

2.   The February 1995 application (which is sometimes referred to as the "Big Book") never clearly explains what it means by "security." It would not be clear to someone of average skill in the field what "secure" means in that application -- for example, with regard to systems, system components, information, or processes. The same is true for such terms as "protected" and "tamper resistant."

3.   If a reasonably skillful computer security professional were to presume that "secure" has all of the attributes that are promised in the February 1995 application, then "secure" requires a guarantee of secrecy, authenticity, integrity, nonrepudiation, and availability, against all security threats identified in that application other than excessively costly brute

force attacks. (What constitutes excessive cost in this context is not clearly explained).

Again taking the February 1995 application's promises for context, "tamper resistance"

requires that some barrier is in place which prevents access to or alteration of information in

an unauthorized manner. The terms "secure" and "security", and additional terms such as

"secure container," "control," "govern," "protect," "protected processing environment," "host

processing environment" and "virtual distribution environment," would be understood, to the

extent possible, as set forth in Microsoft's PLR 4-2 Statement, as opposed to the definitions

listed in InterTrust's PLR 4-2 Statement.

4.   Professor Mitchell will explain the qualifications of a person of reasonable skill in the

computer security field, including as of February 13, 1995, and explain how cited references

(such as U.S. Patent 5,634,012 to Stefik et al., U.S. Patents 4,868,877 and 5,337,360 to

Fischer, Choudhury et al.'s "Copyright Protection for Electronic Publishing over Computer

Networks," U.S. Patent 4,658,093 to Hellman, and Mori et al.'s "Superdistribution: The

Concept and Architecture" (Transactions of the IECE 1990)) would influence such a person's

understanding of the InterTrust disclosure. He may also address the substance of additional

references published or created before February 13, 1995, not cited in the InterTrust patents.

5.   The specifications of the '721, '900, and '861 patents do not resolve any of these

problems with the Big Book application.

Summary of Opinions of Professor David Maier
in Support of Microsoft's Proposed Claim Constructions

1.   The specification of U.S. Patent No. 6,253,193 ("the '193 patent") describes several

mandatory features of the Virtual Distribution Environment ("VDE") architecture, including:

- the creation of a comprehensive data security and commerce world;

- the ability to handle all types of digital works independent of computing platform,
  making it a single, general purpose solution in contrast to multiple, limited purpose
  solutions;

- flexible control mechanisms that can be applied to any granularity of content;

- control mechanisms that are configurable by any user, not just the system designers or
  content providers; and

- isolation of the system programs and protected works from the non-VDE world,
  preventing observation, alteration, interference, or removal from the VDE, except as
  permitted by the VDE control mechanisms.

This does not mean that the capabilities of the Virtual Distribution Environment can be

achieved, only that these are features that the '193 patent makes clear a VDE must have.

2.   The specification of the '193 patent describes a system that requires several

architectural elements including at least the following:

- VDE Foundation Hardware and Software – installed throughout an infrastructure of
  interlinked computing devices;

- The VDE "Secure Container" – a mechanism for packaging protected works, control
  information, and administrative information; and

- The VDE "Control" – a mechanism for defining the regimen for using protected information that is inside a secure container.

3.   Professor Maier will describe the background of a person of ordinary skill in the art. Such a person would understand the claims in light of the required capabilities and architectural features above.

4.   The specification set forth in the '193 patent has numerous inconsistencies in its terminology. Some inconsistencies concern the data hierarchy (e.g., methods, control information, component assemblies). Other examples include the description of a non-secure host event processing environment and the concept of containment.

The following further summarizes Professor Maier's opinions.

I.   **EXPLANATION OF U.S. PATENT NO. 6,253,193**

A.   **Asserted Capabilities of the Virtual Distribution Environment**

The '193 Patent describes a system that is asserted to be the first universal, distributed processing system for persistently controlling digital information. This system was given the name "Virtual Distribution Environment" or "VDE". As described in the Patent, VDE promised at least the following mandatory features:

1. the creation of a comprehensive data security and commerce world;

2. the ability to handle all types of digital works independent of computing platform, making it a single, general purpose solution in contrast to multiple, limited solutions;

3. flexible control mechanisms that can be applied to any granularity of content;

4. control mechanisms that are configurable by any user, not just the system designers or content providers; and

5. isolation of the system programs and protected works from the non-VDE world, preventing observation, interference, or removal from the VDE, except as permitted by the VDE control mechanisms.

Although these features are promised by the '193 Patent, this does not mean that they are necessarily achievable.

1. Comprehensive Data Security and Commerce World

According to the '193 Patent, VDE is described as being the only comprehensive solution in a world of limited solutions. VDE is described as an end-to-end solution for digital works that guarantees the authenticity, confidentiality and integrity of the works and the VDE mechanisms. These protections are promised to be effective against any unauthorized activity by a third party (i.e. a user other than the creator of the work) that has physical possession of the computing hardware and wishes to circumvent the protections.

VDE must provide the ability to control the distribution and usage of digital works as well as tracking, reporting, auditing and handling payment for the distribution and usage. Additionally, VDE must support multiple business models simultaneously, for example, time-based and volume-based charging for the same digital work or licensing digital works with or without added sub-licensing rights.

Only those systems that are members of the electronic commerce world can participate in VDE commerce transactions. Consequently, all transactions must occur between

member systems since there is no way to control digital works that are outside the boundaries of the VDE world.

2. General Purpose

According to the '193 Patent, the VDE system is the only rights management solution needed by its users because it is capable of handling and protecting all types of digital works, such as digital audio, digital video, software, digital cash, digital documents, electronic publications, etc. within a single rights management framework, whereas previous systems handled only limited subsets of information types. It further states that VDE can function within all types of electronic devices, from smart cards, pagers and telephones to supercomputers.

3. Flexible

According to the '193 Patent, the VDE system can manage protected works in arbitrarily sized data chunks, down to the smallest atomic element. The Patent distinguished prior art systems that used access controls that were limited to the file level or resource level. The VDE system is described as being able to meter, track, bill and audit the usage of these arbitrary data chunks in addition to controlling the access to those data chunks. For example, a consumer can be charged by the number of bytes downloaded or by the number of paragraphs printed. Additionally, each of these actions can be specified independently, such that two objects can be metered differently, but billed identically.

This flexibility allows two different users to be charged at different rates, for different granularities, and in different currencies for using the same digital work. The '193 Patent distinguished prior art systems that lacked this flexibility.

4. Controls Configurable by All Users

According to the '193 Patent, the VDE system protects a digital work from the instant it is placed under VDE control subject to the permissions provided by the object creator (or rights holder) at the same or at another VDE "secure node." (The nature of the "secure node" is discussed later.) From that moment, the digital work becomes encapsulated within a VDE container. Then, the creator must grant permissions for accessing and distributing the digital work within the VDE object as well as identify how the object can be handled by other users of the VDE world.

These other users can create additional VDE-based controls for this protected work. In general, these controls only impose additional restrictions on the VDE object because they cannot conflict with the creator's VDE controls (except in the limited case in which the creator allows his controls to be modified by other users.) Even the end user is permitted to add VDE controls to VDE objects that he has received.

VDE controls are said to be persistent in that become permanently associated with the protected work once they are received, and they cannot be removed or deleted except as permitted by so-called "senior" VDE controls.

5. System Isolation

According to the '193 Patent, VDE protected works can only be accessed using VDE-certified foundation hardware and software. As a fundamental requirement, the VDE

Exhibit G – page 7

foundation must isolate the internal workings of the system from the user because the user is not trusted.

Each computing device in the VDE world constitutes a "secure node" that must provide a "protected processing environment" (PPE) composed of VDE-certified foundation hardware and software. Sensitive materials such as protected works, administrative information, control information, and VDE software components, are passed between the protected processing environments of secure nodes inside "secure containers" that shield the materials from outside observation and alteration while in transit or in storage. The PPE must also shield all processing of the materials inside the PPE and also prevent the materials or process state information from "leaving" the VDE except as authorized by VDE control information. If the system fails to keep a protected work secret, then it can be distributed freely from that point onward. If the system fails to prevent alteration, then the consumer may receive invalid information (e.g., a bad stock quote), the consumer may receive less value than that for which he bargained (e.g., digital cash token that has been devalued), or the consumer's computer may be damaged by malicious code (e.g., virus-infected software), just to name a few examples. If the system fails to prevent the materials or process state information from leaving, then it can be moved to a system outside the VDE control regime for examination, manipulation, replication, or analysis.

Electronic devices outside the VDE world do not incorporate the VDE foundation, and hence are not constrained by VDE protocols. Thus, protected works are not permitted to be in clear text form outside of the isolated and rigidly controlled protected processing environment.

Exhibit G – page 8

To guarantee the isolation and integrity of the PPE, the VDE foundation software itself must be protected by storing it in a location that is inaccessible to the user or by encrypting it when it is stored at a location that can be observed by the user.

B.   VDE Core Architecture

According to the '193 Patent, three constituent building blocks are necessary to implement the VDE world:

1. VDE Foundation Hardware and Software – installed throughout an infrastructure of interlinked computing devices, each of which is called a "secure node";

2. The VDE "Secure Container" – a mechanism for packaging protected works, control information, and administrative information; and

3. The VDE "Control" – a mechanism for defining the regimen for using protected information that is inside a secure container.

Both controls and protected works are transferred between secure nodes by means of the secure container mechanism. Secure containers can be opened (and the protected works used) only within the protected processing environment of a secure node by executing VDE controls that regulate and track such activity.

The proper combination of these three building blocks isolates internal processing from the untrusted user (by creating an unbypassable foundation of hardware and software); isolates protected works from the untrusted user (by placing them in a shielded data structure); and provides a control mechanism that will allow the untrusted user to make use of the protected works only under controlled conditions.

1. VDE Foundation Hardware/Software

The VDE foundation hardware and software must ensure that the competing interests of both the owner and user of protected works are respected. The owner has an interest in controlling the distribution of his digital works and in compelling the reporting and payment for such use. The user has an interest in the control of his computing device, his privacy, and the availability of digital works for which he has paid.

The VDE foundation hardware and software must provide a sequestered venue in which external authority dominates the user's local authority in the control of information and processing. This VDE foundation hardware and software is the basis for any VDE installation on a device

A VDE secure node is a device that provides a VDE installation incorporating VDE foundation hardware and software as the base stratum on which all VDE functions are executed. In any secure node where protected works are used or where VDE control information is created or modified, a VDE secure subsystem core must be present. This core is enclosed by a "tamper resistant security barrier" that prevents observation of, interference with, and leaving of information and processes except as authorized by VDE control information.

This VDE secure subsystem core handles encrypting and decrypting data and code, storing control and metering information, managing secure communication with other VDE secure subsystem cores at other secure nodes, dynamically assembling and executing VDE control procedures, and updating control information for protected works.

Control procedures for the promised permission checking, metering, billing, and budget management features all execute within the VDE secure subsystem core.

The VDE foundation hardware and software must guarantee that control procedures triggered by user or system events are executed correctly and completely in the VDE secure subsystem core. Both correctness and completeness are necessary to preserve the integrity of VDE control regime. Failure can compromise the rights, privacy, or financial interests of the owner or user of the protected works.

According to the '193 Patent, these functions are provided and enforced by a secure processing unit (SPU) that is protected by a special purpose physical enclosure (the tamper resistant security barrier) that conceals the underlying VDE processing from observation or interference by external persons or processes, and that destroys information rather than allow the information to leave the VDE subsystem core via unauthorized means.

The '193 Patent suggests that a tamper resistant security barrier might be simulated solely in software by using several known software techniques, but it gives no specific direction as to how these techniques can be applied to achieve the guarantees required by the VDE secure subsystem core in an environment that is under the control of an untrusted user.

2.   VDE Secure Containers

An invariant requirement of the VDE container concept is that no access or use can be made of the protected works within a VDE container except as regulated by associated VDE control information. This associated control information can be provided in the

same secure container that holds the protected works or it can be provided independently in a separate secure container.

In addition to the protected works included within a secure container, there can be references to other digital works stored external to the container. However, the container cannot regulate other access or usage to these externally stored digital works. ("Containment" is discussed further is Section IV. D.)

VDE secure containers can contain administrative information, such as auditing, tracking, and billing requests and reports.

The internal structure of a VDE secure container must be able to store independently manageable digital works. Subsections of a VDE secure container can be encrypted by different keys, including subdivisions of a single digital work.

The internal structure of a VDE secure container must be able to store other VDE secure containers nested inside it. Each nested container is subject to its own independent control information. Control information corresponding to the outer container may not override more restrictive control information that corresponds to a secure container nested within it.

The VDE secure container supports modification of its contents and its control information subject to the current corresponding control information.

Because of this capability, a VDE secure container may be empty in the sense that it does not contain a digital work while it does contain control information that identifies the digital work that can be added to the secure container. Thus, a VDE secure container can be used as a mobile agent to retrieve digital works from remote locations.

3.   VDE Controls

According to the '193 Patent, the configurability and flexibility of the VDE system

arises jointly from the modular and independently selectable nature of control information

and the dynamic construction and execution of control procedures within the VDE secure

subsystem of a computing device. As used herein, the VDE secure subsystem refers to the

VDE foundation hardware and software residing within the tamper resistant security

barrier.

VDE controls are executable procedures constructed by the VDE foundation as a

response to a request to access or use a specific protected work. The control is

constructed inside the VDE secure subsystem using VDE control information. VDE

control information is composed of executable code, rule information that is enforced by

the executable code, and blueprint instructions for constructing the executable control.

The VDE secure subsystem guarantees that the control procedure is constructed according

to the blueprint instructions and that the components used in the construction are authentic

as to source, identity, and data integrity.

All use of protected works is regulated by corresponding control information that is

used to construct each executable control procedure. Different control procedures can

regulate auditing, billing, metering, tracking and usage events (such as printing, rendering,

copying, etc.) with respect to individual users for a single instance of a protected work.

These events cannot occur except as regulated by the execution of the individual control

procedures. Additionally, these control procedures can be applied at arbitrarily fine levels

of granularity, such as charging for the number of bytes read.

Any VDE user can define control procedures to the extent permitted by senior VDE control information.

Control information is deliverable independent of the protected work. Individual portions of control information are deliverable independent of each other. Control information made by added, modified, or replaced over time to the extent permitted by earlier control information. Because independent control information for any given instance of a protected work can be created by different sources at different locations and different times, the control information from these sources can be in conflict. VDE must supply a means for resolving these conflicts. According to the '193 Patent, the executable controls negotiate to determine the conditions under which a protected work may be used. Thus, controls are said to "evolve" over time.

Once delivered to a VDE node with the corresponding protected work, control information persists throughout the life of the protected work.

The VDE controls must support a broad range of control regimes, all of which can co-exist on a single VDE secure node.

Dynamic assembly and execution of a VDE control must occur within the VDE secure subsystem. Construction of a VDE control from its component parts in a non-VDE system allows unconstrained access to digital works. Thus, VDE control information is transmitted between secure nodes using VDE secure containers and stored at VDE nodes in encrypted form whenever outside the VDE secure subsystem.

Executable control procedures are constructed from load modules, data, and VDE methods. These control procedures are assembled and executed in response to user and

system events. According to some statements in the '193 Patent, a "component assembly" is a VDE control procedure.

C.   Claim Interpretation

A person of ordinary skill in the art would understand the claims of the '193 Patent in light of the mandatory capabilities and architectural components described above.

D.   Summary of Internal Inconsistencies.

The '193 Patent contains numerous internal inconsistencies. Examples of these inconsistencies are given below.

1.   Use of Quotations

Hundreds of terms are set off in quotations throughout the specification. These terms include: detail description, virtual distribution environment, electronic highway, VDE aware, content, virtual, things, chain of handling and control, rules and controls, CD ROM, information utility, switch, transaction processor, usage analyst, operating system, method, budget, atomic, firmware, hash bucket, peripheral device, event-based, multi-threaded, locking, Remote Procedure Call, two-phase commit, and read only. Some of these terms are coined (such as VDE aware; rules and controls; and usage analyst) while many are well known computer concepts (such as operating system and Remote Procedure Call.).

In many cases, it is unclear whether any particular use of quotation marks was intended to introduce a coined term, to indicate figurative or metaphorical usage of a term, to indicate non-standard or a weakened usage of a term, or something else

2. System Availability

In the Absract, the '193 Patent asserts that "the invention . . . maintain[s] the integrity, availability, and/or confidentiality" of protected works. However, the system described does not appear to be designed to guarantee the availability of protected works. Rather, any deviation from the expected processing sequence is considered to be evidence of an attempt to crack the system or steal the protected works. In response, the system is likely to halt all processing until a trusted VDE administrator intervenes and resets the system. Additionally, the '193 Patent uses denial of service to enforce reporting obligations imposed by a rights holder. This practice is not consistent with preserving availability of digital works.

3. "Container" vs. "Object"

There is no consistent delineation in the '193 Patent between the terms "container" and "object." Initially, there appears to be a distinction in that the container is a shell data structure that is encapsulating data and the object is the combination of the container data structure and the encapsulated data. See Fig. 5A. Elsewhere, this distinction is blurred by the use of such phrases as:

"secure object (content container)";

"VDE content container is an object"; and

"VDE container (object)",

which appear to make container and object synonymous.

4. The Property of Being "Contained"

In the '193 Patent, there is no clear definition for the term "contain." The '193 patent states at one point that a container such as "container 302 may 'contain' items without those items actually being stored in the container." This definition of "contain" to include "referencing" is not customary in information storage terminology.

Subsequent examples in the '193 indicate that "contain" and "reference" are distinct relationships. For example, "may contain or reference" is used numerous times such as in "Load modules 1100 may contain or reference other load modules." and as in "Container 300y may contain and/or reference. . . ."

5. Inconsistent Data Structure Hierarchy

The hierarchy and relationships amongst rules, controls, methods, load modules, control information, and other data structures is inconsistent.

a) "Rules and Controls" vs. "Control Information"

The term "control information" is defined in the "Background and Summary of the Invention" of the '193 Patent as: ". . . load modules, associated data and methods . . ." Later, the specification uses the phrase " 'rules and controls' (control information)" as if the phrases "control information" and "rules and controls" are synonymous. Further, it states that "rules and controls" can be in the form of: "a 'permissions record' 808; 'budgets' 308 and 'other methods' 1000", but makes no mention of load modules.

Subsequent uses of "control information" such as: ". . . other aspects of the information to be contained within the object (e.g., rules and control information, identifying

information, etc.)"; and "the user may specify permissions, rules and/or control information." indicate that rules are different and distinct from control information.

b) "Component Assembly" vs. "Control Information"

In the '193 Patent, the relationship between component assembly and control information in the data hierarchy is defined inconsistently. Contrast the statement:

"In this example control information may include one or more component assemblies that describe the articles within such a container (e.g. one or more event methods referencing map tables and/or algorithms that describe the extent of each article)."

with:

". . . control information (*typically a collection of methods related to one another by one or more permissions records, including any method defining variables*) . . ." [italics in original]

"This "channel 0" "open channel" task may then issue a series of requests to secure database manager 566 to obtain the "blueprint" for constructing one or more component assemblies 690 to be associated with channel 594 (block 1127). In the preferred embodiment, this "blueprint" may comprise a PERC 808 and/or URT 464.'

In one case, the component assembly is a part of control information, but in the other case, control information is separable from and describes how to build a component assemblies.

c)   "Budgets"

According to the '193 Patent, "budgets" are a special type of "method". Methods are

defined as containing, among other things, "User Data Elements". Elsewhere, budgets are

cited as a common type of User Data Element. This inconsistency creates confusion as to

whether any given use of the term "budget" refers to an executable method or a non-

executable data structure.

6.   "Load Module"

According to the '193 Patent, executable code is provided in the form of "'atomic'

load modules", presumably meaning that they are the smallest unit of executable code.

Later, however, load modules are sub-dividable into smaller load modules, which is

inconsistent with atomicity.

7.   The "Non-Secure" "Protected Processing Environment"

According to the '193 Patent, a necessary feature of a VDE computer is the "protected

processing environment" or "PPE". Secure Event Processing Environments ("SPE"), in

which all sensitive processing is handled inside a hardware device called a Secure

Processing Unit ("SPU") are stated as being one type of PPE. Host Event Processing

Environments ("HPE") are also said to be a type of PPE. The HPE classification is further

described as having two sub-types: secure and non-secure. Additionally, the specification

defines the three abbreviations as synonymous and interchangeable starting at column 103

of the specification, unless the context of any given passage indicates otherwise.

Further, no criteria are provided for distinguishing between a "secure HPE" and a

"non-secure HPE". Thus, it is not possible to reconcile the "non-secure HPE" as a secure

operating environment or protected processing environment.

PROOF OF SERVICE

I am employed in the City and County of San Francisco, State of California in the office of a member of the bar of this court at whose direction the following service was made. I am over the age of eighteen years and not a party to the within action. My business address is Keker & Van Nest, LLP, 710 Sansome Street, San Francisco, California 94111.

On February 3, 2003, I served the following document(s):

PATENT LOCAL RULE 4-3 JOINT CLAIM CONSTRUCTION AND PREHEARING STATEMENT

☑ by **FEDERAL EXPRESS**, by placing a true and correct copy in a sealed envelope addressed as shown below. I am readily familiar with the practice of Keker & Van Nest, LLP for correspondence for delivery by FedEx Corporation. According to that practice, items are retrieved daily by a FedEx Corporation employee for overnight delivery.

Eric L Wesenberg, Esq.
Mark R. Weinstein, Esq.
Orrick Herrington & Sutcliffe
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650/614-7400
Facsimile: 650/614-7401

John D. Vandenberg, Esq.
James E. Geringer, Esq.
Kristin L. Cleveland, Esq.
Klarquist Sparkman Campbell, et al.
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland OR 97204
Telephone: 503/226-7391
Facsimile: 503/228-9446

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Executed on February 3, 2003, at San Francisco, California.

NOELLE S. NICHOLS

305966.01

1 WILLIAM L. ANTHONY (State Bar No. 106908)
   ERIC L. WESENBERG (State Bar No. 139696)
2 MARK R. WEINSTEIN (State Bar No. 193043)
   ORRICK, HERRINGTON & SUTCLIFFE, LLP
3 1000 Marsh Road
   Menlo Park, CA 94025
4 Telephone: (650) 614-7400
   Facsimile: (650) 614-7401
5
   JOHN W. KEKER (State Bar No. 49092)
6 MICHAEL H. PAGE (State Bar No. 154913)
   KEKER & VAN NEST, LLP
7 710 Sansome Street
   San Francisco, CA 94111-1704
8 Telephone: (415) 391-5400
   Facsimile: (415) 397-7188
9
   Additional Counsel Listed at Signature Block
10

11   UNITED STATES DISTRICT COURT

12   NORTHERN DISTRICT OF CALIFORNIA

13   OAKLAND DIVISION

14

15 | INTERTRUST TECHNOLOGIES | Case No. C 01-1640 SBA (MJE)
      CORPORATION, a Delaware corporation,
16   PATENT LOCAL RULE 4-3 JOINT
            Plaintiff,   CLAIM CONSTRUCTION AND
17   PREHEARING STATEMENT
      v.   REVISED IN ACCORDANCE WITH
18   THE SCOPE OF "MINI-*MARKMAN*"
   MICROSOFT CORPORATION, a   HEARING SET FORTH IN THE
19 Washington corporation,   COURT'S ORDER ENTERED 2/24/03

20   Defendant.

21

22 MICROSOFT CORPORATION, a
   Washington corporation,
23
            Counterclaimant,
24 v.

25 INTERTRUST TECHNOLOGIES
   CORPORATION, a Delaware corporation,
26
            Counter Claim-Defendant.
27

28

DOCSSV1:224822.1

In accordance with the Court's Order entered February 24, 2003 and Patent Local Rule 4-3, Plaintiff and Counter-Defendant InterTrust Technologies ("InterTrust") and Defendant and Counter-Claimant Microsoft Corporation ("Microsoft") submit the following revised Joint Claim Construction and Prehearing Statement. Pursuant to that Order, the parties have limited their disputes for purposes of the "Mini-*Markman*" proceeding, to 30 disputed terms and phrases, as identified in alphabetical order in Exhibit B and highlighted in copies of the claims in Exhibit H, hereto.

Submission of "Intrinsic" Evidence

To avoid unnecessary duplication, the parties will submit, prior to the submission of the final briefs in the "Mini-*Markman*" proceeding (including briefing addressing indefiniteness), a Joint Declaration presenting the Intrinsic evidence (including patents, file histories and cited references). The parties agree that in briefs submitted in the "Mini-*Markman*" proceeding, a party may cite to evidence that ultimately will be submitted by the parties in such Joint Declaration and need not append such evidence to a declaration in support of a brief. This agreement does not limit either party from submitting any evidence with a declaration accompanying any brief.

RULE 4-3(a): Agreed Construction

- Attached hereto as **Exhibit I** is a list of claim constructions upon which the parties agree. To the extent that agreed constructions refer to disputed terms that are not among the 30 terms in the "Mini-*Markman*" proceeding, such terms are set forth in quotations.

RULE 4-3(b): Disputed Claim Construction Presentation

- Attached hereto as **Exhibit A** is a list of disputed claim terms set forth in claim order, together with the parties' proposed constructions.
- Attached hereto as **Exhibit B** is a list of the 30 disputed claim terms in alphabetical order, together with the parties' proposed constructions.
- Attached hereto as **Exhibit C** is InterTrust's identification of intrinsic and extrinsic evidence supporting its proposed construction for each of the 30 disputed terms and phrases.

PATENT LOCAL RULE 4-3 JOINT CLAIM
CONSTRUCTION AND PREHEARING
STATEMENT, Case No. C 01-1640 SBA (MEJ)

- Attached hereto as **Exhibit D** is Microsoft's identification of intrinsic and extrinsic evidence supporting its proposed construction for each of the 30 disputed terms and phrases.

- Attached hereto as **Exhibit E** is a Microsoft statement of reservations.

- Attached hereto as **Exhibit H** is the text of the 12 claims at issue, with bolding identifying the terms and phrases in dispute for the purposes of the "Mini-*Markman*" proceeding.

RULE 4-3(c): Claim Construction Hearing Length

The claim construction schedule is set forth in the Court's Order entered February 24, 2003.

RULE 4-3(d): Witness Testimony

The parties have agreed to present witness testimony through declarations filed in support of the briefs. There also shall be tutorial presentations, per the Court's Order of February 24, 2003.

- Attached hereto as **Exhibit F** is a summary of expert testimony to be presented by InterTrust.

- Attached hereto as **Exhibit G** is a summary of expert testimony to be presented by Microsoft.

RULE 4-3(e): Pre-Hearing Conference Issues

The parties addressed pre-hearing matters at the Case Management Conference hearing on February 13, 2003. No pre-hearing conference is currently scheduled or requested.

Dated: March 14, 2003

INTERTRUST TECHNOLOGIES
CORPORATION
MARK SCADINA - #173103
JEFF MCDOW - #184727
4800 Patrick Henry Drive
Santa Clara, CA 95054
Telephone: (408) 855-0100
Facsimile: (408) 855-0144

By: _____ *FOR JEFF McDow*
    Jeff McDow

1
2
3
4
5
6
7
8 Dated: March 14, 2003
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

KEKER & VAN NEST, LLP
MICHAEL H. PAGE

DERWIN & SIEGEL
DOUGLAS K. DERWIN - #111407
3280 Alpine Road
Portola Valley, CA 94028
Telephone: (650) 529-8700
Facsimile: (650) 529-8799

Attorneys for Plaintiff and Counter-Defendant
INTERTRUST TECHNOLOGIES
CORPORATION
WILLIAM L. ANTHONY
HEIDI L. KEEFE
MARK R. WEINSTEIN
ORRICK, HERRINGTON & SUTCLIFFE LLP

By: _____
     Sam O'Rourke

KLARQUIST SPARKMAN, LLP
One World Trade Center
121 S.W. Salmon, Suite 1600
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Microsoft Corporation

PATENT LOCAL RULE 4-3 JOINT CLAIM
CONSTRUCTION AND PREHEARING
STATEMENT, Case No. C 01-1640 SBA (MEJ)